TD ALGEBRE

LICENCE

NICE 78-79

IMSP 1978-79

M1 UV algèbre et arithmétique.
Feuille N° 1

Horaire des T.D: Groupe 1 Mardi 15h45 – 17h15 Salle 1.1
Mercredi 8h45 – 10h15 " "

Groupe 2 Mardi 14h – 15h30 Salle 1.1
Mercredi 10h30 – 12h " "

Exercices

× 1°/ Soit G un groupe. Donner une condition nécessaire et suffisante pour que la réunion de sous-groupes H et K de G soit un sous-groupe de G.

× 2°/ L'intersection, la réunion et la différence symétrique sont elles des lois de groupe sur l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E (même vide!)?

× 3°/ Soit G un groupe. On considère la loi de composition interne définie sur $\mathcal{P}(G)$ = ensemble des parties de G par

$$(A, B) \longmapsto AB = \{ ab \mid a \in A \text{ et } b \in B \}$$

α) Vérifiez qu'elle n'induit pas une loi de composition interne sur l'ensemble des sous-groupes de G.

β) Si H et K sont des sous-groupes de G, prouvez que HK est un sous-groupe de G si et seulement si $HK = KH$.

γ) Trouvez un groupe G et deux sous-groupes H et K de G tels que HK ne soit pas un sous-groupe de G.

δ) Si G est un groupe commutatif, $(A, B) \longmapsto AB$ est-elle une loi de groupe sur l'ensemble des sous-groupes de G?

✓ 4°/ a) Soit H le sous-ensemble de $Gl(\mathbb{C}^2)$ formé des matrices de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{C}^*$ dites homothéties de $\mathbb{C}^2$. Vérifiez que H est un sous-groupe distingué de $Gl(\mathbb{C}^2)$.

Le groupe $\mathbb{P}Gl(\mathbb{C}^2) = Gl(\mathbb{C}^2)/_H$ est appelé le groupe linéaire projectif de $\mathbb{C}^2$.

b) Soit $Sl(\mathbb{C}^2)$ le sous-ensemble de $Gl(\mathbb{C}^2)$ défini par

$$m \in Sl(\mathbb{C}^2) \iff \det m = 1$$

Prouvez que $Sl(\mathbb{C}^2)$ est un sous-groupe distingué dans $Gl(\mathbb{C}^2)$, dit groupe spécial linéaire de $\mathbb{C}^2$.

c) On définit les sous-ensembles $Gl^+(\mathbb{R}^2)$ et $Gl^-(\mathbb{R}^2)$ de $Gl(\mathbb{R}^2)$ par $m \in Gl^+(\mathbb{R}^2) \iff \det m > 0$

$$m \in Gl^-(\mathbb{R}^2) \iff \det m < 0.$$

Sont-ce des sous-groupes distingués de $Gl(\mathbb{R}^2)$?

× 5°/ Soit E un espace vectoriel sur un corps commutatif k. Montrer que le centre de $Gl(E)$ (i.e l'ensemble des automorphismes qui commutent avec tous les autres) est l'ensemble des homothéties de E de rapport non nul.

× 6°/ Soient n et m deux entiers supérieurs à 1. Etudiez $Hom(\mathbb{Z}, \mathbb{Z})$, $Hom(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ et $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$; (on remarquera qu'un homomorphisme est défini, ici, par la valeur qu'il prend en 1)

7°/ Soit G le groupe (à vérifier, après avoir défini une loi...) des transformations bijectives affines de $\mathbb{R}$ (i.e des applications $f : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = ax + b$, $a \neq 0$).

Montrez que l'ensemble H des homothéties (multiplication par un scalaire) est un sous-groupe ~~distingué~~ non distingué de G, et que le groupe G/H est isomorphe au groupe des translations.

Montrer que le groupe des translations T est un sous-groupe distingué de G.

①

Montrons que

$$\{H \cup K = \text{s. groupe de } G\} \Longleftrightarrow \{H \subset K \text{ ou } K \subset H\}$$

($\Leftarrow$) évident.

($\Rightarrow$) Supposons, par l'absurde, que $\begin{cases} H \not\subset K \\ \text{et} \\ K \not\subset H \end{cases} \Longleftrightarrow \begin{cases} \exists x \in H \setminus K \\ \exists y \in K \setminus H \end{cases}$

Comme la loi . est interne dans H, $xy \in H \cup K$. Supposons, par exemple (ce qui ne restreint pas la généralité) que $xy \in H$.

● Alors $xy = h \in H \Rightarrow y = \underbrace{x^{-1}}_{\in H}\underbrace{h}_{\in H} \Rightarrow y \in H$

Or $y \in K \setminus H$, d'où l'absurdité.

② Considérons $\mathcal{P}(E)$

a) $(\mathcal{P}(E), \cap) \neq$ groupe ~~abélien~~ (pas d'élément symétrique) sauf si ~~E~~ $E = \emptyset$

$(\underbrace{\mathcal{P}(\emptyset)}_{=\{\emptyset\}}, \cap) =$ groupe commutatif

b) $(\mathcal{P}(E), \cup) \neq$ groupe

$\emptyset =$ le "prétendant" élément neutre

● Soit $A \neq \emptyset$ $A \in \mathcal{P}(E)$. Soit A' tel que $A \cup A' = \emptyset$ (si A' existe)

mais $A \cup A' \supset A \Rightarrow A \cup A' \neq \emptyset \quad \forall A'$

$\nexists A^{-1}$

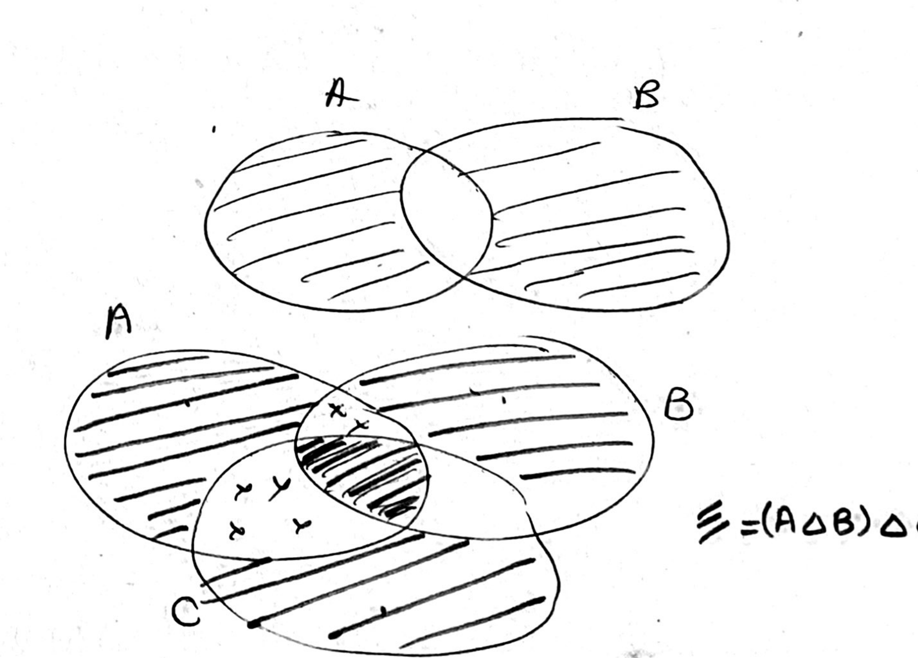
c) $(\mathcal{P}(E), \Delta)$

$= (A \cup B) \cap \complement(A \cap B)$

$A \Delta B = (A \setminus B) \cup (B \setminus A)$

$= (A \cup B) \setminus (A \cap B)$

* Δ est interne
* associatif



1- méthode

$A \Delta B = (A \cap \bar{B}) \cup (\bar{A} \cap B)$

$(A \Delta B) \Delta C = \{ [(A \cap \bar{B}) \cup (\bar{A} \cap B)] \cap \bar{C} \} \cup \{ \overline{[(A \cap \bar{B}) \cup (\bar{A} \cap B)]} \cap C \}$

$= \{ (A \cap \bar{B} \cap \bar{C}) \cup (\bar{A} \cap B \cap \bar{C}) \} \cup \{ [(\bar{A} \cup B) \cap (A \cup \bar{B})] \cap C \}$

$[(B \cap A) \cup (\bar{A} \cap \bar{B})] \cap C$

$[(\bar{A} \cap \bar{B} \cap C) \cup (A \cap B \cap C)]$

$(A \Delta B) \Delta C = (A \cap \bar{B} \cap \bar{C}) \cup (\bar{A} \cap B \cap \bar{C}) \cup (\bar{A} \cap \bar{B} \cap C) \cup (A \cap B \cap C)$

$A \Delta (B \Delta C) = (B \Delta C) \Delta A = (B \cap \bar{C} \cap \bar{A}) \cup (\bar{B} \cap C \cap \bar{A}) \cup (\bar{B} \cap \bar{C} \cap A) \cup (B \cap C \cap A)$ } =

donc $\boxed{(A \Delta B) \Delta C = A \Delta (B \Delta C)}$

2- méthode $\quad \chi_A$ = fct caractéristique de A

$\chi_{(A \Delta B) \Delta C} \overset{?}{=} \chi_{A \Delta (B \Delta C)}$

$\chi_{A \Delta B}(x) = (\chi_A(x) - \chi_B(x))^2$

=

donc :

$\chi_{A \Delta (B \Delta C)}(x) = (\chi_A(x) - (\chi_B(x) - \chi_C(x))^2)^2$

= on développe

3- méthode $\quad \chi : E \longrightarrow \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

$x \longmapsto \chi(x) = \begin{cases} 0 \text{ si } x \notin A \Delta B \\ 1 \text{ si } x \in A \Delta B \end{cases}$

Alors $\chi_{A \Delta B} = \chi_A + \chi_B$

A B x

d'où $\chi_{A \Delta (B \Delta C)} = \chi_{(A \Delta B) \Delta C} \Rightarrow A \Delta (B \Delta C) = (A \Delta B) \Delta C$

* $A \Delta B = B \Delta A$
* $\forall A \in \mathcal{P}(E) \quad A \Delta \emptyset = A$
* $\forall A \quad \exists A' \, / \quad A \Delta A' = \emptyset$ On prend $A' = A$.

Remarque

$$A \overset{\varphi}{\longmapsto} \chi_A$$

$$(\mathcal{P}(E), \Delta) \longrightarrow (\mathcal{F}(E, \mathbb{Z}/2\mathbb{Z}), +)$$

φ = isomorphisme car
* $\varphi(A \Delta B) = \chi_{A \Delta B} = \chi_A + \chi_B = \varphi(A) + \varphi(B)$
* φ bijective (facile)

On peut aussi munir $\mathbb{Z}/2\mathbb{Z}$ de la loi . qui fait que $(\mathbb{Z}/2\mathbb{Z}, +, .)$ = anneau.

Alors $(\mathbb{Z}/2\mathbb{Z})^E$ = anneau.

Alors

$$\varphi : (\mathcal{P}(E), \Delta, \cap) \longrightarrow ((\mathbb{Z}/2\mathbb{Z})^E, +, .)$$

$$A \longmapsto \chi_A$$

est un isomorphisme d'anneau.

En effet : $\varphi(A \cap B) = \chi_{A \cap B} = \chi_A . \chi_B = \varphi(A) . \varphi(B)$

(3)

G = groupe
$(A, B) \mapsto AB = \{ ab \, / \, a \in A \text{ et } b \in B \}$

α) et γ)

$\mathcal{S}_3$ = groupe des permutations d'un ensemble à 3 éléments.
(Il y a 6 éléments, et c'est le plus petit qui soit non commutatif)

jusqu'à 5, tous commutatifs } $\mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Z}/3\mathbb{Z}$ $\quad \mathbb{Z}/5\mathbb{Z}$ $\longrightarrow$ $\forall G$ à p el.) p premier G isom. à $\mathbb{Z}/p\mathbb{Z}$ (cf. cours)

$\mathbb{Z}/4\mathbb{Z}$ non iso. à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein)

Rappels

$\mathcal{S}_3$: liste des sous-groupes

$H \subset \mathcal{S}_3$, alors $\# H = 2$ ou 3

* si $ord(H) = 6$, $H = \mathcal{S}_3$
* si ordre $H = 3$ $\quad H = \{1, (1\,2\,3), (1\,3\,2)\}$
* si ordre $H = 2$ $\quad \{1, (1\,2)\} \quad \{1, (1\,3)\} \quad \{1, (2\,3)\}$
* si $ord(H) = 1$, $H = \{1\}$

(Remarque : Pro 1 : $ord(G) = p$ premier $\Rightarrow$ G isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Pro 2 : G iso à $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow \exists a \in G \quad G = \langle a \rangle$)

Retour au γ)

Prenons $H = \{1, (1\,2)\}$

$K = \{1, (1\,3)\}$

$$HK = \{1, (1\,2), (1\,3), (1\,3\,2)\}$$

et $HK \neq$ sous-groupe de $\mathcal{S}_3$ (il sont tous répertoriés dans les rappels !)

β) H et K sous-groupes de G ;

HK est un sous-groupe de G $\Leftrightarrow$ HK = KH

Preuve :

($\Rightarrow$) (Par l'absurde) supposons que HK soit un sous-groupe et que $HK \neq KH$

$$HK \neq KH \Leftrightarrow \begin{cases} HK \not\subset KH \Leftrightarrow \exists h \ \exists k \ \forall h' \ \forall k' \quad hk \neq k'h' & (1) \\ \text{ou} \\ KH \not\subset HK \Leftrightarrow \exists h \ \exists k \ \forall h' \ \forall k' \quad kh \neq h'k' & (2) \end{cases}$$

(notations évidentes)

* Si (1) a lieu, considérons $(hk)^{-1}$.

$(hk)^{-1} \in HK$ car HK = sous-groupe

Mais alors : $\exists h' \in H \quad \exists k' \in K \;/\; (hk)^{-1} = h'k'$

$\Updownarrow$

$hk = k'^{-1} h'^{-1}$

faux (cf (1))

~~Si (2) a lieu, on considerera $(kh)^{-1}$~~ :

$(~~kh~~)^{-1}$

~~* Si ¬(1) a lieu~~.

* Si (1) n'a pas lieu, alors $HK \subset KH$ et (2) a lieu.

Prenons h et k définis en (2).

$$\left.\begin{array}{l} h \in HK \\ k \in HK \end{array}\right\} \Rightarrow kh \in HK \Rightarrow (kh)^{-1} \in HK \subset KH$$

(HK sous-groupe)

donc : $\exists h' \in H \quad \exists k' \in K \;/\; (kh)^{-1} = k'h'$

$\Updownarrow$

$kh = (h'^{-1})(k'^{-1})$

ce qui contredit (2)

(NB : démonstration directe derrière cette feuille)

$(\Leftarrow)$ $HK \neq \emptyset$ puisque $e \in HK$

$\forall a \in HK \; \forall b \in HK$ Montrons que $ab^{-1} \in HK$

$$\left\{\begin{array}{l} a = hk \\ b = h'k' \end{array}\right. \Rightarrow ab^{-1} = h\underbrace{k\,k'^{-1}\,h'^{-1}}_{\in KH = HK}$$

$$ab^{-1} = \underbrace{h\,h_1}_{\in H} k_1 \Rightarrow ab^{-1} \in HK \text{ vrai.}$$

démonstration directe $(\Rightarrow)$

* $KH \subset HK$

En effet : $\forall k \in K \quad \forall h \in H \qquad (kh)^{-1} = h^{-1}k^{-1} \in HK$ sous-groupe

$$\Downarrow$$

$$kh \in HK$$

* $HK \subset KH$

$\forall h \in H \quad \forall k \in K \qquad (hk)^{-1} \in HK$ (= sous-groupe)

$$\Updownarrow$$

$\exists h' \in H \quad \exists k' \in K \qquad k^{-1}h^{-1} = h'k'$

$$hk = k'^{-1}h'^{-1} \in KH$$

donc $HK \subset KH$

δ) On suppose que G est abélien. Alors la loi $(A,B) \mapsto AB$ est bien une loi interne dans l'ensemble des groupes.

* Associativité

$(AB)C = A(BC)$ oui

* élément neutre

Notons $E = \{e\}$ Alors $EA = AE = A$ ceci $\forall A$ groupe de G.

* élément symétrique

Soit A

• Si

$\neq e$

E

• Si

= oui.

Conclusion

• Si $G \neq \{e\}$, montrons que G n'admet pas de sym.

$\exists a \in G \setminus \{e\}$

$\forall B$ sous-groupe de $G \quad a \in \overset{G}{AB} \Rightarrow \overset{G}{AB} \neq \{e\} = E$

G n'est pas inversible.

• Si $G = \{e\}$, $\forall A$ sous-groupe de G, $A = G$

et $A = G = E$.

Alors la loi × (qui n'a plus aucun intérêt !) est une loi de groupe dans l'ens. des sous-groupes de E (il n'y en a pas des masses)

Extension de la question 8)

exo || Soit G groupe et H une partie finie de G
|| Alors $e \in H$ et H stable $\Rightarrow$ H sous-groupe (I)

(cf tout anneau intègre fini est un corps) (II)

lemme.

Lemme : Soit G un ensemble muni d'une loi interne, associative et possédant un élément neutre.

Soit H partie finie, $H \ni e$, et stable.

Alors tout élément régulier de H est symétrisable

En effet :

$x \in H$ régulier

$f : H \to H$

$y \mapsto xy$

* f injective car $xy = xy' \Rightarrow y = y'$

* H fini et $f : H \to H \Rightarrow$ f surjective.

Donc : $\exists x' \in H \ / \ f(x') = e = xx'$ et x est inversible.

→ Application à (I)

→ Application à (II)

A anneau int.

$G = A \setminus \{0\}$

⑤ $(GL(E), \circ)$ = groupe $E = K$-e.v.

Th | Soit $h \in GL(E)$
h est une homothétie ~~de ra~~ ssi $\forall D$ droite vectorielle de E

$$h(D) = D$$

(démonstration : voir exposé cap. sur les homothéties)

Soit H l'ensemble des homothétie, et notons Z le centre de $GL(E)$

* On a $H \subset Z$

* Inversement, montrons que $Z \subset H$

Soit $f \in Z$

$\forall u \in GL(E)$ $f \circ u = u \circ f$

Soit D droite vect. de E, quelconque.

$\exists s \in GL(E)$ symétrie vect. par rapport à D // à un plan quelconque.

$$f \circ s = s \circ f$$

$\forall x \in D$ $f(x) = s(f(x))$

$\Updownarrow$ ← Attention, si K de caractéristique $\neq 2$
Sinon, prendre une affinité.

$f(x) \in D$

$f(D) \subset D$ $f \in GL(E) \Rightarrow f(D) = D$

Donc f = homothétie.

(4)

c) $GL(\mathbb{R}^2) \xrightarrow{\Psi} \{-1, 1\}$

$u \longmapsto \dfrac{\det u}{|\det u|} = \operatorname{Sgn}(\det u)$

Ψ est un morphisme de groupe, et $\operatorname{Ker}\Psi = \{u \in GL(\mathbb{R}^2) \,/\, \det u > 0\} = GL^+(\mathbb{R}^2)$

Ainsi GL^+ = sous-groupe distingué.

Remarque

Th | $\forall H \triangleleft G \quad \exists G'$ groupe tel que $\varphi : G \to G' \,/\, H = \operatorname{Ker}\varphi$

Preuve :

On prend $G' = G/_H$ et φ = surjection canonique.

---

(5)

Attention : la démonstration faite en algèbre utilisant les symétries s par rapport à des droites est dangereuse car elle suppose que le corps sur lequel on travaille est de caractéristique différente de 2

E = e.v. sur K

$E = D \oplus P$

s = symétrie / à D parallèlement à P.

Alors $\operatorname{Inv} s = \{x \in E \,/\, s(x) = x\} = D \iff K$ est un corps de caractéristique $\neq 2$

$\longrightarrow$ la démonstration se fait bien, quand m̂, avec une affinité de rapport λ.

2-solution

Montrons que $Z \subset H$.

Soit $h \in Z \quad \forall u \in GL(E) \quad h \circ u = u \circ h$

Montrons que h laisse invariant les droites.

Contraposée : ~~Soit~~ $\exists a \,/\, a \neq 0 \quad a \in E \;/\; (a, h(a))$ soit libre.

Soit F le plan vectoriel engendré par $(a, h(a))$, et G tel que $F \oplus G = E$

Soit u telle que $\begin{cases} u|_G = Id \\ u|_F \text{ définie par } \begin{cases} u(a) = a \\ u(h(a)) = a + h(a) \end{cases} \end{cases}$. $u \in GL(E)$

Alors u ne commute pas avec h. En effet :

$$\begin{cases} (u \circ h)(a) = u(h(a)) = a + h(a) \\ (h \circ u)(a) = h(a) \end{cases} \Rightarrow u \circ h(a) \neq h \circ u(a)$$

CQFD

(6)

Soient G, G' 2 groupes, et $Hom(G, G')$. <u>G' abélien</u>

$$(fg)(x) = f(x)g(x)$$

* $(Hom(G, G'), .)$ = groupe ?

$$(fg)(xy) = f(xy)\,g(xy) = f(x)f(y)\,g(x)\,g(y)$$
$$= f(x)g(x)\,f(y)g(y)$$
$$= (fg)(x)\,(fg)(y)$$

Notons $(G', +)$, $(G, .)$. fg est défini par :

$$(fg)(x) = ~~f(x)g(x)~~\ f(x) + g(x)$$

<u>Exercice</u>

<u>$Hom(\mathbb{Z}, G)$</u>

Soit $f \in Hom(\mathbb{Z}, G)$ $\quad f : \mathbb{Z} \to G$

$0 \mapsto 0$

$1 \mapsto f(1) = a \in G$

$\vdots$

$n \mapsto f(n) = na$ (par récurrence)

où na est défini par $\begin{cases} 0a = 0 \\ 1a = a \\ na = (n-1)a + a \end{cases}$

<u>Remarque</u> On a ainsi défini la loi interne $\mathbb{Z} \times G \to G$, $(n, a) \mapsto na$

qui vérifie $\begin{cases} 1a = a \\ n(a+b) = na + nb \\ (n+m)a = na + ma \\ 0a \end{cases}$

On dit que G a une structure de <u>module sur $\mathbb{Z}$</u>.

~~Alors~~ :

Réciproquement, $\begin{aligned} f : \mathbb{Z} &\to G \\ n &\mapsto na \end{aligned}$ est un homomorphisme

$$\text{Hom}(\mathbb{Z}, G) = \{ f : \mathbb{Z} \to G \quad \exists a \in G \quad \forall n \in \mathbb{Z} \quad f(n) = na \}$$

<u>Remarque</u>

Montrer que $\begin{aligned} \varphi : \text{Hom}(\mathbb{Z}, G) &\longrightarrow G \\ f &\longmapsto a = f(1) \end{aligned}$

est un ~~hom~~ isomorphisme de groupe.

On peut ainsi identifier $\text{Hom}(\mathbb{Z}, G)$ et G.

<u>$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$</u>

Soit $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}$ (f morphisme)

$\dot{0} \longmapsto 0$

$\dot{1} \longmapsto f(\dot{1})$

$0 \leq k \leq n-1$ $\quad \dot{k} \longmapsto k f(1)$

~~$\dot{n} \longmapsto$~~

Mais $\begin{cases} f(\dot{n}) = n f(\dot{1}) \\ \text{et} \\ f(\dot{n}) = f(\dot{0}) = 0 \end{cases}$ donc $n f(\dot{1}) = 0 \Rightarrow f(\dot{1}) = 0$

$$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$$

<u>$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$</u> ?

Cherchons $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$ (G abélien)

$\simeq \{ x \in G \,/\, nx = 0 \}$

G = groupe abélien (noté +)
Montrer que $\mathrm{Hom}(\mathbb{Z}/_{n\mathbb{Z}}, G) \simeq \overbrace{\{x \in G \,/\, nx = 0\}}^{A}$

Soit $f \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$

$$\begin{aligned} f : \mathbb{Z}/_{n\mathbb{Z}} &\to G \\ 0 &\mapsto 0 \\ 1 &\mapsto f(1) \\ &\vdots \\ 0 = n &\mapsto f(n) = n f(1) = f(0) = 0 \end{aligned} \Rightarrow n f(1) = 0. \Rightarrow f(1) \in A$$

Considérons $\varphi : \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \longrightarrow A$
$f \longmapsto f(1)$

- φ = homomorphisme de groupes $\quad \varphi(f+g) = (f+g)(1) = \varphi(f) + \varphi(g)$
- φ injective, car, pour $f(1)$ fixé $\in A$, $f(p) = p f(1)$ $\forall p \in \mathbb{Z}/n\mathbb{Z}$ $\Rightarrow f$ unique.
- ~~φ surjective~~ : ~~$\forall x \in A$~~ $\exists f$ ~~$\in \mathbb{Z}/n\mathbb{Z}$~~ morphisme de ~~$\mathbb{Z}/n\mathbb{Z} \to G$~~. ~~$f(x) = xp$~~ $f(1) = x$ $\{$ ~~$\forall p \in \mathbb{Z}/n\mathbb{Z}$~~ on a $f(p) = px \}$

(2)

- φ surjective. Soit $x \in A$. Montrons qu'il existe $f \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$ telle que $\varphi(f) = x \Leftrightarrow f(\dot{1}) = x$

problème →

On définit f par : $\forall \xi \in \mathbb{Z}/n\mathbb{Z} \quad \exists k \,/\, \xi = \dot{k} \quad f(\xi) = kx$

Cette écriture défini bien f puisque : $\xi = \dot{k} = \dot{k'} \Rightarrow \begin{cases} f(\xi) = kx \\ f(\xi) = k'x \end{cases}$

et $k' - k = nq \Rightarrow f(\xi) = kx = (k' - nq)x = k'x - q\underbrace{(nx)}_{0}$
$= f(\xi')$.

Cas où $\mathbb{Z}/_{m\mathbb{Z}} = G$

On doit chercher $A = \{\dot{x} \in \mathbb{Z}/m\mathbb{Z} \,/\, n\dot{x} = \dot{0}\}$ (x = "un" représentant de $\dot{x}$)

$n\dot{x} = \dot{0} \Leftrightarrow m \mid nx \Leftrightarrow \frac{m}{\delta} \Big| \frac{n}{\delta} x \quad$ où $\Delta(m,n) = \delta$

$\Leftrightarrow \frac{m}{\delta} \Big| x \quad$ (cf. th. de Gauss et $\Delta(\frac{m}{\delta}, \frac{n}{\delta}) = 1$)

$\Leftrightarrow x \in \frac{m}{\delta}\mathbb{Z} \Leftrightarrow \exists \lambda \in \mathbb{Z} \,/\, \dot{x} = \lambda \dot{\left(\frac{m}{\delta}\right)}$

d'où $\quad A = m'\left(\mathbb{Z}/m\mathbb{Z}\right) \quad$ où $m = \delta m'$

$$A = m'\left(\mathbb{Z}/m'\delta\mathbb{Z}\right) \simeq \mathbb{Z}/\delta\mathbb{Z} \qquad \text{(cf lemme)}$$

$$\boxed{A \simeq \mathbb{Z}/\delta\mathbb{Z}}$$

<u>lemme</u> : $\quad p\left(\mathbb{Z}/pq\mathbb{Z}\right) \simeq \mathbb{Z}/q\mathbb{Z}$

$$\underbrace{p\left(\mathbb{Z}/pq\mathbb{Z}\right)}_{\substack{\cup\!\!\!\!\mid \\ \xi}} \longrightarrow \mathbb{Z}/q\mathbb{Z}$$

$\exists\, \bar{\xi} \in \mathbb{Z}/pq\mathbb{Z} \ /\ p\bar{\xi} = \xi$

$\exists\, x \in \mathbb{Z} /\ \bar{\xi} = \dot{x}$

$$\left\{ \begin{array}{l} \xi \overset{\varphi}{\longmapsto} \bar{x} \qquad \text{(classe de } x \text{ modulo } q\text{)} \\ \text{où } \ \xi = p\dot{x} \qquad\qquad (\dot{x} = \text{classe de } x \text{ modulo } pq) \end{array} \right.$$

Peut-on définir φ comme cela ?

$$\xi = p\dot{x'} = p\dot{x} \overset{?}{\Rightarrow} \bar{x} = \bar{x}' \ ?$$

oui car $\quad p\dot{x}' = p\dot{x} \iff px' - px \in \mathbb{Z}/pq\mathbb{Z}$

$$\iff x' - x \in \mathbb{Z}/q\mathbb{Z}$$

$$\iff \bar{x} = \bar{x}'$$

- φ bien définie
- φ = homomorphisme bijectif

<u>Remarque</u> : Le lecteur vérifiera que l'isomorphisme de $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ vers $\mathbb{Z}/\delta\mathbb{Z}$ (où $\delta = \Delta(m,n)$) est

$$f \longmapsto \frac{1}{m'} f(1) \qquad\qquad (\delta m' = m)$$

$$\boxed{\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/_{\Delta(m,n)}\mathbb{Z}}$$

<u>Prolongement</u> : $\mathrm{Aut}(\mathbb{Z}/_{n}\mathbb{Z})$?

⑦ • $H = \{ h \in G \,/\, h(x) = \alpha x \}$

1) $(G, \circ)$ = groupe

2) $(G, \circ) \xrightarrow{\varphi} (\mathbb{R}^*, \times)$

$f = ax + b \longmapsto a$

morphisme $\quad \mathrm{Ker}\,\varphi = \{ f \in G \,/\, a = 1 \} = T$

donc :

• $G/_T \simeq \mathrm{Im}\,\varphi$ et $\mathrm{Im}\,\varphi = (\mathbb{R}^*, \times) \simeq$ (Homothéties, $\circ$)

donc $G/_T \simeq (H, \circ)$ $\quad$ (H = ensemble des homothéties)

UNIVERSITÉ DE NICE
INSTITUT DE MATHÉMATIQUES
ET SCIENCES PHYSIQUES
PARC VALROSE
06034 NICE CEDEX
TÉL. (93) 51.91.00
MATHÉMATIQUES

M 1 Algèbre et arithmétique

Feuille N°2

× 1° On munit l'ensemble $\mathbb{R}$ de la loi de composition

$$(x,y) \longmapsto \sqrt[3]{x^3+y^3}$$

Montrer qu'on obtient ainsi un groupe isomorphe à $(\mathbb{R},+)$. Plus généralement, si G est un groupe et φ une bijection de G sur un ensemble X, définir un groupe isomorphe à G par φ et dont l'ensemble sous-jacent soit X. Y a-t-il plusieurs solutions ?

× 2° Trouver tous les groupes à 1, 2, 3, 4, 5, 6, 7 éléments.

× 3° Soit G un groupe. Pour tout $a \in G$, on définit une application $s_a : G \to G$ par $S_a(x) = ax$ (translation à gauche d'amplitude a). Montrer que $a \mapsto S_a$ est un isomorphisme de G sur un groupe de permutation de G. Corollaire ?

v 4° Deux éléments x et y d'un groupe G sont dits conjugués s'il existe un $s \in G$ avec $y = sxs^{-1}$. Montrer que la conjugaison est une relation d'équivalence dans G.

×5°) Étant donné une partie A d'un groupe G, et $s \in G$, on note sAs^{-1} l'ensemble $\{sas^{-1} \mid a \in A\}$. Montrer que si A est un sous-groupe, il en est de même de sAs^{-1}, qu'on appelle un sous-groupe conjugué de A. Le normalisateur $N(A)$ d'un sous-groupe A de G est l'ensemble $\{s \in G \mid sAs^{-1} = A\}$. Montrer que $N(A)$ est un sous-groupe (distingué ?) de G et que le centre de A est un sous-groupe distingué de $N(A)$.

v × 6°) Soit G un groupe, à un élément $a \in G$ on associe l'"automorphisme intérieur" σ_a de G défini par $\sigma_a(x) = axa^{-1}$.

α) montrer que $\sigma_a \in \mathrm{Aut}\, G$

β) montrer que $a \mapsto \sigma_a$ est un morphisme de groupes de G dans $\mathrm{Aut}\, G$, Quel est son noyau ?

7°) Montrer que si deux sous-groupes H et K d'un groupe G sont d'indice fini, il en est de même de $H \cap K$ [plonger $G/_{H\cap K}$ dans $G/_H \times G/_K$]. Montrer que si $H \cap L$ et $K \cap L$ sont d'indice fini dans G, il en est de même de $H \cap K$.

8°) Quel est l'indice de $Gl^+(\mathbb{R}^2) = \{m \in Gl(\mathbb{R}^2) \mid \det m > 0\}$ dans le groupe $Gl(\mathbb{R}^2)$.

9°) Montrer que $\Gamma_n = \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$. A quelle condition Γ_n est-il un sous-groupe de Γ_m ? Déterminer $\Gamma_n \cap \Gamma_m$ et le sous-groupe engendré par $\Gamma_n \cup \Gamma_m$?

① 1°/ On définit la loi interne $*$ sur $\mathbb{R}$ par $x * y = \sqrt[3]{x^3+y^3}$

Pro | $\varphi : (\mathbb{R},+) \longrightarrow (\mathbb{R},*)$
$x \longmapsto \sqrt[3]{x}$ est un morphisme surjectif pour les lois $+$ et $*$.

Preuve :

- $\varphi(x+y) = \varphi(x) * \varphi(y)$
- φ est surjective (et même bijective)

Donc $(\mathbb{R},*)$ = groupe (cf. rappel ci-dessous)

Rappel : Th | G, H deux ensembles munis respectivement des lois internes $.$ et $*$
Soit $f : G \to H$ un morphisme surjectif pour ces lois.
Alors : $(G,.)$ = groupe $\Rightarrow$ $(H,*)$ = groupe

Preuve : On a $f(xy) = f(x) * f(y)$

- A $(f(x) * f(y)) * f(z) = f(xyz) = f(x) * (f(y) * f(z))$
- N $f(x) * f(e) = f(e) * f(x) = f(e)$
- S $(f(x))^{-1} = f(x^{-1})$

2°/ Soit $(G,.)$ un groupe, et soit $\varphi : G \to X$ bijective.

a) S'il existait une loi $*$ donnant à X une structure de groupe rendant l'application φ isomorphe, on aurait forcément $\varphi(x) * \varphi(x') = \varphi(xx')$ (1)

b) Posons, par définition : $\forall y, y' \in$ $y * y' = f(xx')$ où $\begin{cases} y = f(x) \\ y' = \varphi(x') \end{cases}$

- On peut définir $*$ ainsi, car $\varphi(xx')$ est unique une fois x et x' fixés (car φ bijective)
- On vérifie que cette loi $*$ ainsi définie est bien une loi de groupe sur X.

D'où le théorème (Transport des structures par une bijection)

Th | Soient $(G,.)$ un groupe, X un ensemble et φ une bijection de G sur X
Alors il existe une unique loi $*$ structurant $(X,*)$ en groupe rendant l'application φ isomorphe de $(G,.)$ sur $(X,*)$.
Cette loi est définie par : $\varphi(x) * \varphi(y) = \varphi(xy)$

② Trouver tous les sous-groupes à 1, 2, 3, 4, 5, 6, 7 éléments.

Soit G un groupe d'ordre n.

• $G = \{e\}$

• ~~G isomorphe à $\mathbb{Z}/2\mathbb{Z}$. En Cela résulte~~

Alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. G est donc un groupe monogène.

$$G = \{e, a\} \quad \text{où } a^2 = e$$

Cela provient des théorèmes :

Th | Tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Th | G est un groupe monogène $\Leftrightarrow$ G est un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$

On résoud ainsi facilement les cas où n est premier :

- $n = 2$ G isomorphe à $\mathbb{Z}/2\mathbb{Z}$
- $n = 3$ G " $\mathbb{Z}/3\mathbb{Z}$
- $n = 5$ G " $\mathbb{Z}/5\mathbb{Z}$
- $n = 7$ G " $\mathbb{Z}/7\mathbb{Z}$

• <u>$n = 4$</u> $G = \{e, a, b, c\}$ e, a, b, c tous distincts entre eux

$\langle a \rangle$ = groupe d'ordre p, et p divise ord(G) = 4.
donc $p = 2$ ou 4 (si $p = 1$, $a = e$ faux)

De 2 choses l'une :

* Si $\forall x \in G$ $\#\langle x \rangle = 2$, alors $G = \{e, a, b, c\}$ où $a^2 = e$, $b^2 = e$, $c^2 = e$

La table d'un tel groupe est :

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Alors $G \sim \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein)

* Si $\exists x \in G$ $\text{ord}\langle x\rangle = 4$. $G = \{e, a, a^2, a^4\} \sim \mathbb{Z}/4\mathbb{Z}$

• $n=6$ $G = \{e, a, b, c, d, f\}$

a) $\exists x \in G \,/\, \text{ord}\langle x\rangle = 6$, alors $G \sim \mathbb{Z}/6\mathbb{Z}$

b) $\forall x \in G$ $\text{ord}\langle x\rangle \neq 6$

■ Lemme | Soit G, et a tel que $\text{ord}\langle a\rangle = p$ premier
Alors $x \in \langle a\rangle$ et $x \neq e \Rightarrow \langle x\rangle = \langle a\rangle$

Preuve :

On a $x \in \langle a\rangle \Rightarrow \langle x\rangle \subset \langle a\rangle$, et $\underbrace{\text{ord}\langle x\rangle}_{\neq 1} \mid \text{ord}\langle a\rangle = p \Rightarrow \text{ord}\langle x\rangle = \text{ord}\langle a\rangle$

Ainsi $\begin{cases} \langle x\rangle \subset \langle a\rangle \\ \text{ord}\langle x\rangle = \text{ord}\langle a\rangle \end{cases} \Rightarrow \langle x\rangle = \langle a\rangle$

■ Pro | 1) G possède au moins un élément d'ordre 2
2) " au moins un élément d'ordre 3

Preuve :

1) S'il n'y avait que des éléments d'ordre 3 : $G = \{e, \underbrace{a, \underset{b}{a^2}, c, \underset{d}{c^2}}, f \ldots$ plus de place pour f^2
tous distincts (voir lemme)

2) S'il n'y avait que des éléments d'ordre 2

■ Notons $\begin{cases} \tau \text{ notre élément d'ordre } 2 \\ \sigma \text{ notre élément d'ordre } 3 \end{cases}$

	e	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
e	e	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	e	$\tau\sigma^2$ (1)	τ	$\tau\sigma$
σ^2	σ^2	e	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	e	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	e	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	e

← tous distincts (le vérifier)

$\boxed{\tau\sigma^2 \ (1)}$ ~~[illegible]~~ 1 : • $\sigma\tau \neq e, \sigma, \sigma^2, \tau$.

• Si $\sigma\tau = \tau\sigma$, alors $\omega(\sigma\tau) = 6$ ($\omega(x)$ = ordre de x) ce qui est impossible.

On sait que $(\sigma\tau)^6 = e$. Reste à montrer que 6 est le p. petit nombre n / $(\sigma\tau)^n = e$.

$n = 2$ ou 3. * $(\sigma\tau)^2 = \sigma^2\tau^2$ (car $\sigma\tau = \tau\sigma$)

$= \sigma^2 \neq e$

* $(\sigma\tau)^3 = \tau \neq e$

• Donc $\boxed{\sigma\tau = \tau\sigma^2}$

On a remarqué qu'il n'y avait qu'une façon de faire la table de multiplication. Or, je connais S_3 qui est à 6 él. et qui possède 1 él. d'ordre 2 et 1 él. d'ordre 3. Donc $G \sim S_3$.

<u>Moralité</u>

ord $G = 6$ ↗ $G \sim \mathbb{Z}/6\mathbb{Z}$

ord $G = 6$ ↘ $G \sim S_3$

③ $S_a : G \to G$
$x \mapsto ax$

Soit $S : G \to \mathcal{S}_G$
$a \mapsto S_a$

* $S_a \in \mathcal{S}_G$ car S_a est un homomorphisme
De plus S_a est bijectif, puisque : $\forall y \in G \ \exists! x \ / \ ax = y$ à savoir $x = a^{-1}y$

* S est un homomorphisme, puisque $\forall a, a' \in G \quad \forall x \in G \quad S_{aa'}(x) = aa'x$

$$= a(a'x)$$
$$= S_a \circ S_{a'}(x)$$

S est injectif, puisque : $\text{Ker } S = \{a \in G \ / \ \forall x \in G \ \ ax = x\} = \{e\}$

$\text{Im } S$ = sous-groupe de $\mathcal{S}_G$

Corollaire : Tout groupe est isomorphe à un sous-groupe d'un groupe de permutations

$$G \simeq \text{sous-groupe de } \mathcal{S}_G$$

⑤ G, A sous-groupe de G

$N(A) = \{ s \in G \ / \ sAs^{-1} = \sigma_s(A) = A \}$

- $N(A) \neq \emptyset$
- $s, t \in N(A) \Rightarrow \sigma_{st}(A) = A$?

On a $\sigma_{st}(A) = \sigma_s(\sigma_t(A)) = \sigma_s(A) = A$ donc $st \in N(A)$

- $s \in N(A) \Rightarrow s^{-1} \in N(A)$

$N(A)$ = sous-groupe.

N(A) distingué ?

Si A distingué $N(A) = G$ puisque $\forall x \in G \quad xAx^{-1} = A \Rightarrow x \in N(A)$
distingué dans G

Contre exemple

$\begin{cases} G = \mathcal{S}_3 & \text{(plus petit sous-groupe non commutatif)} \\ A = \{1, \tau\} & (\tau = \text{transposition}) \end{cases}$

(A est bien un sous-groupe non distingué car, si σ = autre transposition, $\sigma\tau\sigma^{-1} \neq Id$ et $\sigma\tau\sigma^{-1} \neq \tau$ car autrement $\sigma\tau = \tau\sigma \Rightarrow$ le sous-groupe engendré par $\{\sigma$ et $\tau\}$ serait $\{1, \sigma, \tau, \sigma\tau\}$ d'ordre 4, qui ne divise pas 6 !)

~~$s \in N(A) \Leftrightarrow \begin{cases} s \dots s^{-1} = 1 \\ s\tau s^{-1} = \tau \end{cases}$~~

On a $\underbrace{A}_{\text{ordre } 2} \subset \underbrace{N(A)}_{\text{ordre } n} \subset \underbrace{\mathcal{S}_3}_{\text{ordre } 6} \Rightarrow 2 | n$ et $n | 6 \Rightarrow n = 2$ ou 6

Or $n \neq 6$, sinon $N(A) = G \Rightarrow A \triangleleft G$ faux.

Remarque : Règle de calculs.

$s \tau s^{-1}$ et $\tau = (a_0, \dots, a_n)$
Alors $s\tau s^{-1} = (s(a_0), \dots, s(a_n))$

On montre que $\begin{cases} s|_{\{s(a_0), \dots, s(a_n)\}} = s\tau s^{-1}|_{\{s(a_0), \dots, s(a_n)\}} \\ s|_{\complement\{s(a_0), \dots, s(a_n)\}} = Id \end{cases}$

$Z \triangleleft N(A)$

1-démonstration

Z = centre de $A = \{z \in A \,/\, \forall x \in A \quad zx = xz\}$

Z = sous-groupe distingué de $N(A)$ car :

- $Z \subset N(A)$ trivial
- Z = sous-groupe trivial
- Z distingué dans $N(A)$?

$\forall z \in Z \quad \forall s \in N(A) \quad szs^{-1} \in Z$?

On a : $\forall x \in A \quad szs^{-1} x = szx's^{-1}$ où $s^{-1}xs = x' \in A$ (car $s \in N(A)$)

$= sx'zs^{-1}$ car $x'z = zx'$ ($x' \in A$ $z \in Z(A)$)

$szs^{-1}x = x''szs^{-1}$ où $sx's^{-1} = x'' \in A$ (car $s \in N(A)$)

Or : $x'' = sx's^{-1} = s(s^{-1}xs)s^{-1} = x$

d'où : $\forall x \in A \quad (szs^{-1})x = x(szs^{-1}) \Leftrightarrow szs^{-1} \in Z$

CQFD

2- démonstration

On a $\left.\begin{array}{l} Z(A) \lhd\lhd A \\ A \subset N(A) \text{ et } A \lhd N(A) \end{array}\right\} \Rightarrow Z(A) \lhd N(A)$

| où : $H \lhd\lhd G \Leftrightarrow \forall u \in Aut(G) \quad u(H) \subset H$
| cf théorème $H \lhd\lhd G \lhd L \Rightarrow H \lhd L$

Remarque : "le normalisateur $N(A)$ est le plus grand sous-groupe de G dans lequel A est distingué".

Preuve : $A \lhd H \subset G \Rightarrow H \subset N(A)$

$\Updownarrow \qquad \Updownarrow$

$\forall t \in H \quad \sigma_t(A) = A \Rightarrow \forall t \in H \quad t \in N(A)$

(7) $H \subset G$

L'indice du groupe H dans G est, par définition

$$[G : H] = Card(G/_H) \underset{(1)}{=} Card({}_H\backslash G)$$

[(1) : En effet $\exists$ bijection $G/_H \longrightarrow {}_H\backslash G$

$xH \longmapsto Hx^{-1}$

car : $xH = x'H \Leftrightarrow Hx^{-1} = Hx'^{-1}$

$\Updownarrow \qquad \Updownarrow$

$x^{-1}x' \in H \Leftrightarrow x'x^{-1} \in H$]

Exercice

a) $G/_H$ et $G/_K$ finis $\Rightarrow G/_{H\cap K}$ fini

Soit φ : $G/_{H\cap K} \longrightarrow G/_H \times G/_K$

$(H\cap K)x \longmapsto Hx \times Kx$

Existe ? $(H\cap K)x = (H\cap K)x'$

$$\Updownarrow$$

$$xx'^{-1} \in H\cap K$$

$$\Updownarrow$$

$$\begin{cases} xx'^{-1} \in H \\ \text{et} \\ xx'^{-1} \in K \end{cases} \Leftrightarrow \begin{cases} Hx = Hx' \\ \\ Kx = Kx' \end{cases}$$

ce qui montre, d'un coup, que φ est définie et est injective

CQFD

b) $G/_{H\cap L}$ fini et $G/_{K\cap L}$ fini $\Rightarrow$ $G/_{H\cap K}$ fini.

D'après le a), on a $G/_{H\cap L}$ fini et $G/_{K\cap L}$ fini $\Rightarrow G/_{H\cap K\cap L}$ fini.

Or $\varphi : G/_{H\cap K\cap L} \xrightarrow{\text{surj.}} G/_{H\cap K}$ est définie et surjective.

$$(H\cap K\cap L)x \longmapsto (H\cap K)x$$

définie : $(H\cap K\cap L)x = (H\cap K\cap L)x' \Leftrightarrow xx'^{-1} \in H\cap K\cap L \subset H\cap K$
$\Rightarrow (H\cap K)x = (H\cap K)x'$

surjectivité : $\exists x\in G \;/\; \xi = (H\cap K)x \Rightarrow \xi = \varphi(x(H\cap K\cap L))$

donc $G/_{H\cap K}$ fini.

(8)

On sait que $Gl^+(\mathbb{R}^2) = \{m \in Gl(\mathbb{R}^2) \;/\; \det m > 0\}$ est un sous-groupe distingué de $Gl(\mathbb{R}^2)$ (cf. $\varphi : Gl(\mathbb{R}^2) \to \{-1,1\}$, $m \mapsto \frac{\det m}{|\det m|}$)

$\text{ord}\left(Gl(\mathbb{R}^2)/Gl^+(\mathbb{R}^2)\right)$?

$$\begin{array}{ccc} Gl(\mathbb{R}^2) & \xrightarrow{\varphi} & \{-1,1\} \\ \pi \downarrow & \nearrow \tilde{\varphi} = \text{isomorphisme.} & \\ Gl(\mathbb{R}^2)/Gl^+(\mathbb{R}^2) & & \end{array}$$

car $\text{Ker}\,\varphi = Gl^+(\mathbb{R}^2)$

Donc $\text{ord}\left(Gl(\mathbb{R}^2)/_{Gl^+(\mathbb{R}^2)}\right) = 2$ (cf. orientation d'un e.v.)

(9) $n \neq 0$ $\quad \Gamma_n = \{ z \in \mathbb{C} \ / \ z^n = 1 \}$

Γ_n = sous-groupe de $\mathbb{C}^*$ (c'est le noyau de $(\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$, $z \mapsto z^n$)

(NB : Γ_n isomorphe à $\mathbb{Z}/n\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z} \to \Gamma_n$, $k \mapsto e^{i\frac{2\pi k}{n}}$

Pro | $\Gamma_n \subset \Gamma_m \Leftrightarrow n \mid m$

($\Rightarrow$) Γ_n = sous-groupe de $\Gamma_m \Rightarrow n \mid m$

($\Leftarrow$) $m = nq \Rightarrow z^n = 1 \Rightarrow z^m = 1$

Pro | $\Gamma_n \cap \Gamma_m = \Gamma_{\Delta(m,n)}$

En effet $\Gamma_n \cap \Gamma_m = \{ z \in \mathbb{C}^* \ / \ z^n = z^m = 1 \}$ (par ex. $n \leq m$)

→ si $n \mid m$. $\Gamma_n \cap \Gamma_m = \Gamma_n$

→ si $n \nmid m$ $\quad m = nq + r \quad r < n$

$z^n = z^{nq+r} = 1 \Leftrightarrow \underbrace{z^n = z^r = 1}$

{ si $r \mid n$ $\quad \cap = \Gamma_r$
{ sinon, on continue

On obtient ainsi une suite strictement ↓ (dans $\mathbb{N}$) qui converge

~~donc~~ donc
$$\begin{cases} m = nq + r \\ n = rq_1 + r_1 \\ \text{----} \\ r_{k+1} = \underbrace{r_{k+2}}\, q_{k+3} + 0 \end{cases}$$
dernier reste non nul

et $\Delta(m,n) = r_{k+2}$
⇓
$\Gamma_n \cap \Gamma_m = \Gamma_{r_{k+2}}$

← (algorithme d'Euclide)

$$\boxed{\Gamma_n \cap \Gamma_m = \Gamma_{\Delta(m,n)}}$$

Remarque : autre démonstration.

‖ Si G = sous-groupe fini de $\mathbb{C}^*$, alors $G = \Gamma_n$ où $n = \# G$

(voir th. cours)

Preuve : Soit $z \in G$ $\quad z^n = 1 \Rightarrow G \subset \Gamma_n$
or $\# \Gamma_n = n$
$\Rightarrow \Gamma_n = G$

$z \in \Gamma_n \cap \Gamma_m \Leftrightarrow (z^d)^{n'} = (z^d)^{m'} = 1$ où $\Delta(m', n') = 1$, $\begin{cases} m = m'd \\ n = n'd \end{cases}$

$\Leftrightarrow z^d \in \Gamma_{n'} \cap \Gamma_{m'}$

(NB) Corps des quaternions $\mathbb{H}$

1- définition $1, i, j, k$ base de $\mathbb{H}$

x dans $\mathbb{Q}$ 1 neutre $i^2 = j^2 = k^2 = -1$; $ij = k$, $ki = j$; $jk = i$

$a + bi + cj + dk$ $\quad ij = -ji$, $ki = -ik$, $jk = -kj$

2- façon géométrique ($\wedge$)

C'est le plus petit corps non commutatif

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ (1950) : il n'y a pas de corps entre, ni après.

Suite : $z^d \in \Gamma_{n'} \cap \Gamma_{m'}$ (1)

$\Gamma_{n'} \cap \Gamma_{m'}$ = sous-groupe fini de $\mathbb{C}^* \Rightarrow \exists \; \Gamma_{n'} \cap \Gamma_{m'} = \Gamma_{d'}$

et $\Gamma_{d'} \subset \Gamma_{n'} \Rightarrow d' | n'$
$\Gamma_{d'} \subset \Gamma_{m'} \Rightarrow d' | m'$ $\Big\} \Rightarrow d' = 1$ ($\delta(m', n') = 1$)

(1) $\Leftrightarrow$ donc $z^d \in \Gamma_{d'} = \Gamma_1$

$(z^d)^1 = 1 = z^d$

$\Downarrow$

$\Gamma_n \cap \Gamma_m \subset \Gamma_d$

La réciproque est vraie car $d | n$ et $d | m \Rightarrow \Gamma_d \subset \Gamma_n \cap \Gamma_m$

autre démonstration

$$\mathbb{N}^* \longrightarrow \underbrace{\{\text{ss groupes finis de } \mathbb{C}^*\}}_{\eta}$$
$$n \longmapsto \Gamma_n$$

- elle est bijective (réciproque : $\#G \longleftarrow G$)
- $(\mathbb{N}^*, |)$ $\quad (\eta, \subset)$
  ↑ ordre $\quad$ ↑ ordre

l'application est croissante car $n | m \Rightarrow \Gamma_n \subset \Gamma_m$

C'est un isomorphisme pour la relation d'ordre ($\Leftrightarrow$ bijection croissante)

$\mathbb{N}^* \longrightarrow \eta$

$n, \quad m$ — Γ_n, Γ_m

$d = \Delta(m,n)$ le plus grand div. commun à n et m

Γ_d = le plus grand sous-groupe commun à Γ_m et Γ_n

$\Downarrow$

$\Gamma_d = \Gamma_m \cap \Gamma_n$

b) $<\Gamma_n \cup \Gamma_m>$ $\quad (\mathbb{N}^*, |) \longrightarrow (\eta, \subset)$

n, m

$<\Gamma_n \cup \Gamma_m>$ = le plus petit sous-groupe de $\mathbb{C}^*$ contenant $\Gamma_n \cup \Gamma_m$.

p = le plus petit multiple commun à n et m.

$\left.\begin{array}{l}\Gamma_n \subset \Gamma_{mn} \\ \Gamma_m \subset \Gamma_{mn}\end{array}\right\} \Rightarrow <\Gamma_n \cup \Gamma_m>$ = sous-groupe fini.

Γ_{mn} fini

← - - - - on traduit

donc $<\Gamma_n \cup \Gamma_m> = \Gamma_p$

UNIVERSITÉ DE NICE
INSTITUT DE MATHÉMATIQUES
ET SCIENCES PHYSIQUES
PARC VALROSE
06034 NICE CEDEX
TÉL. (93) 51.91.00
MATHÉMATIQUES

M1 Algèbre et Arithmétique.

Feuille d'exercices N°3

× 1°) Montrer que $\mathfrak{S}_4$ possède un sous-groupe distingué isomorphe au groupe de Klein.

× 2°) Montrer que pour deux sous-groupes H et G de Γ, $H \triangleleft \Gamma$ et $G \triangleleft H$ n'implique pas $G \triangleleft \Gamma$.

× 3°) Montrer qu'un sous-groupe d'indice deux est distingué.

× 4°) Quels sont les sous-groupes maximaux de $\mathbb{Z}/n\mathbb{Z}$?

× 5°) Soient a et b dans $\mathbb{Z}$
Si $(a,b)=1$, montrer qu'il existe $u, v \in \mathbb{Z}$ vérifiant $ua+vb=1$ avec $|u|<|b|$ et $|v|<|a|$. Unicité ?

× 6°) Quels sont les éléments d'ordre 2 de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$? Quels sont ceux d'ordre 4 ? Trouver tous les automorphismes de $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ [Pour $a, b \in G$ avec $\omega(a)=2$, $\omega(b)=4$, l'application $f: G \to G$ définie par $f(\dot{x},\dot{y}) = xa+yb$ est linéaire]

× 7°) Déterminer $\mathrm{Aut}(\mathfrak{S}_3)$, $\mathrm{Aut}(\mathcal{K})$, munir $\mathfrak{S}_3 \times \mathcal{K}$ d'une structure de groupe isomorphe à $\mathfrak{S}_4$.

× 8°) Déterminer le groupe $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ [préciser pour $n = 2, 3, 4, 5, 7, 8, 13, 15, 21, 24$]

× 9°) Montrer, de deux façons différentes que

$$\frac{(2a)!\,(2b)!}{a!\,b!\,(a+b)!}$$ est un entier.

× 10°) Si $a_1, \dots a_n \in \mathbb{Z}$ vérifient $\sum_{i=1}^{n} a_i = 0$, montrer que pour tout nombre premier p, $\text{Min}\{v_p(a_i) \mid 1 \le i \le n\}$ est atteint au moins deux fois. Montrer que $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ n'est jamais entier pour $n > 1$ [Observer que $v_2(x)$ pour $x = 1, 2, \dots, n$ atteint une fois son maximum]

AS

11°) Les suites $[an]$, $[bn]$, $n \in \mathbb{N}$ représentent* une fois et une seule les entiers (traduire !) si et seulement si $a, b \notin \mathbb{Q}$, $a, b > 0$ et $\frac{1}{a} + \frac{1}{b} = 1$.

d'où $H \simeq H'$ ⇏ $G/H \simeq G/H'$ ne pas confondre $\simeq$ et $=$!

× 13°) Trouver un groupe G, deux sous-groupes H et H' de G, isomorphes, et tels que G/H et G/H' non isomorphes.

× 14°) Montrer que le nombre de diviseurs de $a \in \mathbb{N}$ est impair si et seulement si a est un carré.

4. XII. 78

---

* c.à.d $a, b \in \mathbb{R}$ (a_n) (b_n) $\forall x \in \mathbb{R}$ $\exists!\, n$

Existence

(5) $\Delta(a,b)=1$

$\exists u_0, v_0 \,/\, au_0 + bv_0 = 1$ (équation de Bezout)

On sait résoudre l'équation (1) à inconnues $u, v \in \mathbb{Z}$:

$$(1) \quad au + bv = 1$$

$$(1) \Leftrightarrow \exists q \in \mathbb{Z} \begin{cases} u = u_0 + bq \\ v = v_0 - aq \end{cases}$$

On veut trouver $q \in \mathbb{Z}$ tel que $\begin{cases} |u| < |b| \\ \text{et} \\ |v| < |a| \end{cases} \Leftrightarrow \begin{cases} |u_0 + bq| < |b| \\ |v_0 - aq| < |a| \end{cases}$

Or :
$$\begin{cases} \exists!\, q \in \mathbb{Z} \quad \exists!\, r \in \mathbb{Z} \quad u_0 = (-b)q + r \quad \text{où} \quad |r| < \frac{|b|}{2} & (2) \\ \exists!\, q' \in \mathbb{Z} \quad \exists!\, r' \in \mathbb{Z} \quad v_0 = aq' + r' \quad \text{où} \quad |r'| < \frac{|a|}{2} & (3) \end{cases}$$

Prenons $r = u$ et $r' = v$. Pour que (u,v) soit solution de (1), il suffira que $q = q'$.

Montrons donc que $q = q'$.

$$au_0 + bv_0 = 1 \Leftrightarrow a(-bq + u) + b(aq' + v) = 1$$
$$\Leftrightarrow au + bv + ab(q' - q) = 1$$
$$\Leftrightarrow au + bv = 1 - ab(q' - q) \qquad (4)$$

Si $q \neq q'$ $|(q'-q)| \geq 1 \Rightarrow \underbrace{|au + bv|}_{<|ab|} = |1 - ab(q'-q)|$

~~$\geq |ab|q$~~

$\geq |1 - |ab(q'-q)||$

$\geq |ab(q'-q)| - 1$

$\geq |ab| - 1$

$> |ab|$

d'où la contradiction.

Donc $q = q' \Rightarrow \begin{cases} u = u_0 + bq \\ v = v_0 - aq \end{cases}$ (u,v) sol. de (1) et $\begin{cases} |u| < |b| \\ |v| < |a| \end{cases}$

CQFD

(5) $\exists u_0, v_0 \,/\, au_0 + bv_0 = 1$ $\quad$ $a, b \neq \pm 1$ $\quad$ $(\delta(a,b)=1)$

$u_0 = bq + u \qquad 0 < u < |b|$

d'où $a(bq+u) + bv_0 = 1 \Leftrightarrow au + b(\underbrace{v_0 + aq}_{v}) = 1$

A-t-on $|v_0 + aq| < |a|$?

$|v_0 + aq| < |a| \Leftrightarrow |1 - au| < |ab|$

~~vrai car $|au - 1| < ||ab| + 1|$~~

donc $|v| \leq \frac{1}{|b|} + |a|$ dans $\mathbb{Z}$, donc $|v| \leq |a|$

et $|v| \neq |a|$ sinon ...

donc $v < |a|$

Pas unicité $\quad 2.3 + (-1)5 = 1$

$(-3)3 + 2.5 = 1$

Remarque : Pour les polynômes, il y a unicité, alors qu'il n'y avait pas unicité dans $\mathbb{Z}$!

$\delta(P,Q) = 1 \qquad \exists U, V \,/\, UP + VQ = 1$ et $\begin{cases} \deg U < \deg Q \\ \deg V < \deg P \end{cases}$

$\begin{cases} U'P + V'Q = 1 \\ UP + VQ = 1 \end{cases} \Leftrightarrow (U' - U)P = (V - V')Q$

d'après le théorème de Gauss : $Q \mid U' - U$ et $\deg(U' - U) < \deg Q \Rightarrow U' = U$.

CQFD

(Cela provient de : on peut faire augmenter la valeur absolue de $a - b$, alors qu'on ne peut pas faire augmenter le degré de $P - Q$.)

(6) $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ n'est pas cyclique car $\delta(2,4) \neq 1$.

$\omega(\dot{a}, \bar{b}) = \text{ppcm}(\omega(\dot{a}), \omega(\bar{b}))$ d'où :

$(\dot{0}, \dot{0})$ d'ordre 1 $\qquad (1, 0)$ d'ordre 2

$(0,1)$ " 4 $\qquad (1,1)$ " 4

$(0,2)$ " 2 $\qquad (1,2)$ " 2

$(0,3)$ " 4 $\qquad (1,3)$ " 4

Soit

$f : G \to G$

$(\dot{x}, \dot{y}) \mapsto x\dot{a} + y\dot{b}$ où $\begin{cases} \omega(\dot{a}) = 2 \\ \omega(\dot{b}) = 4 \end{cases}$

f est bien définie, car :

Si $\begin{matrix} \dot{x} = \dot{x}' \\ \dot{y} = \dot{y}' \end{matrix}$, on a : $x\dot{a} + y\dot{b} = x'\dot{a} + y'\dot{b}$

puisque $\underbrace{(x - x')}_{2k} a = \underbrace{(y' - y)}_{4q} b$

$ \; 0 \qquad\qquad 0$

f est un automorphisme de G car : * f est un morphisme

* f bijective ? Pas toujours.

① Soit $K = \{1, (12)(34), (13)(24), (23)(14)\}$

K possède tous les éléments de $\mathcal{S}_4$ décomposables en produit de 2 cycles de longueur 2, puisqu'il y a 6 transpositions distinctes de $\mathcal{S}_4$. C'est un sous-groupe de $\mathcal{S}_4$ ⇒ ≃ au groupe de Klein.

Montrons que $K \triangleleft \mathcal{A}_4$ et que $K \triangleleft \mathcal{S}_4$

1°/ $K \triangleleft \mathcal{A}_4$

- K est bien un sous-groupe de $\mathcal{A}_4$, puisque $\text{Sgn}\,\sigma = 1$ $(\forall \sigma \in K)$
- $\forall \sigma \in K \quad \forall \tau \in \mathcal{A}_4 \qquad \tau\sigma\tau^{-1} \in K$

En effet, $\tau\sigma\tau^{-1}$ = conjugué de σ ⇔ $\tau\sigma\tau^{-1}$ et σ sont décomposables en cycles de m̂ longueur 2-2

⇓

$\tau\sigma\tau^{-1} \in K$

2°/ $K \triangleleft \mathcal{S}_4$

- K = sous-groupe de $\mathcal{S}_4$, isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\forall \sigma \in K \quad \forall \tau \in \mathcal{S}_4 \quad \tau\sigma\tau^{-1} \in K$ (m̂ démonstration qu'au 1°/), donc K distingué dans $\mathcal{S}_4$

② Contre-exemple : (la relation de distinction n'est pas transitive)

$A \triangleleft B \triangleleft C \not\Rightarrow A \triangleleft C$

Soient $\mathcal{S}_4$, $K = \{1, (12)(34), (13)(24), (24)(13)\}$ et $A = \{1, (12)(34)\}$

a) $\left\{\begin{array}{l} A \subset K, \text{ K commutatif car} \simeq \text{groupe de Klein} \\ A = \text{sous-groupe de } K \end{array}\right. \Rightarrow A \triangleleft K$

b) On a vu au ① que $K \triangleleft \mathcal{S}_4$

c) Montrons que, pourtant, A n'est pas distingué dans $\mathcal{S}_4$.

Nous avons : $(132)[\underbrace{(12)(34)}_{\in A}](123) = (24) \notin A$

CQFD

③ $\text{ord}\, G/H = 2 \Rightarrow G/H = \{H, G\setminus H\}$

$\forall x \notin H \qquad Hx = G\setminus H \qquad (1)$

$\text{ord}\, G/H = \text{ord}\ {}_H\backslash G \Rightarrow {}_H\backslash G = \{H, G\setminus H\}$

$\forall x \notin H \qquad xH = G\setminus H \qquad (2)$

(1) et $(2) \Rightarrow \forall x \notin H \quad xH = Hx$

Exercice Suppl

$m \geq 1$

Alors $\{x \in \mathbb{N}^* \ / \ \varphi(x) = m\}$ est borné. (donc fini)

$x = \prod p_i^{r_i} \qquad r_i > 0$

$\varphi(x) = \prod p_i^{r_i - 1}(p_i - 1) = x \prod \left(1 - \frac{1}{p_i}\right)$ en fonction de $\frac{1}{\varphi(x)}$?

~~on a~~ ; $\frac{1}{x}$ ~~—~~ $\prod \frac{p_i - 1}{p_i}$ ~~—~~ $\varphi(x)$

$\varphi(x) \prod \frac{p_i - 1}{p_i} = \prod \frac{p_i - 1}{p_i} p_i^{r_i - 1}(p_i - 1) = \prod (p_i - 1)^2 p_i^{r_i - 2}$ *

Que dire de $(p-1)^2 p^{r-2} = \delta$?

$r \geq 2 \Rightarrow \delta = (p-1)^2 p^{r-2} \geq 1$

$r = 1 \Rightarrow \delta = (p-1)^2 \frac{1}{p} = p - 2 + \frac{1}{p}$

si $p \geq 3 \quad \delta \geq 1$

si $p = 2 \quad \delta = \frac{1}{2}$

Donc : ~~$\forall r, \forall p$~~

$\forall r \geq 1$

$\begin{cases} \forall p > 2 & \delta \geq 1 \\ p = 2 & \delta \geq \frac{1}{2} \end{cases}$

Donc $\prod (p_i-1)^2 p_i^{\alpha_i - 2} \geqslant \frac{1}{2} \Rightarrow \prod \frac{p_i - 1}{p_i} \geqslant \frac{1}{2\varphi(n)} \Rightarrow \frac{\varphi(n)}{n} \geqslant \frac{1}{2\varphi(n)}$

d'où $\boxed{n \leqslant 2(\varphi(n))^2}$

Rappels : Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Soit G un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, alors $\pi^{-1}(G)$ est un sous-groupe de $\mathbb{Z}$ contenant $\pi^{-1}(\dot{0}) = n\mathbb{Z}$. Posons $\pi^{-1}(G) = d\mathbb{Z} \supset n\mathbb{Z}$ (*)

Nous aurons $\pi(d\mathbb{Z}) = G$ (car π est surjective)

Pro | Il existe une bijection entre les diviseurs de n (d) et les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ ($\pi(d\mathbb{Z})$)

Preuve :

- A chaque diviseur d de n on fait correspondre le sous-groupe $\pi(d\mathbb{Z}) \subset \mathbb{Z}/n\mathbb{Z}$.
- Cette application est surjective par construction (cf (*))
- Injectivité ?

Montrons que $\left.\begin{array}{l}\pi(d\mathbb{Z}) = \pi(d'\mathbb{Z}) \\ d|n \text{ et } d'|n\end{array}\right\} \Rightarrow d = d'$

Nous avons : $\pi(d) \in \pi(d'\mathbb{Z}) \Leftrightarrow \exists a \in \mathbb{Z} \,/\, d - d'a \in n\mathbb{Z}$

$\Leftrightarrow \exists a \in \mathbb{Z} \,/\, n \mid (d - d'a)$

$\Leftrightarrow \exists b \; \exists a \,/\, d - d'a = bn$

or $\left.\begin{array}{l} d'|n \Rightarrow d'|d \\ \text{de } \hat{m} : \; d|d' \end{array}\right\} \Rightarrow d = d'$. oui

Remarque $\pi(d\mathbb{Z}) = \{\xi \in \mathbb{Z}/n\mathbb{Z} \,/\, \exists x \in \mathbb{Z} \quad \xi = dx\} = d(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$

(4) Sous-groupes maximaux de $\mathbb{Z}/n\mathbb{Z}$

$G \subset \mathbb{Z}/n\mathbb{Z}$ est maximal $\Leftrightarrow \left\{ \begin{array}{c} G \subset H \subset \mathbb{Z}/n\mathbb{Z} \\ \Downarrow \\ H = G \text{ ou } H = \mathbb{Z}/n\mathbb{Z} \end{array} \right.$

1-méthode

Soit G maximal, alors $\exists ! d$ $\quad d | n$ et $G = \pi(d\mathbb{Z})$

Soit H / $G \subset H \subset \mathbb{Z}/n\mathbb{Z}$ $\quad \exists ! d' | n$ / $H = \pi(d'\mathbb{Z})$

et $\quad \pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Rightarrow \underbrace{\pi^{-1}(\pi(d'\mathbb{Z}))}_{= d'\mathbb{Z}} \supset \underbrace{\pi^{-1}(\pi(d\mathbb{Z}))}_{= d\mathbb{Z}}$ (cf. lemme)

Lemme : on a toujours $d\mathbb{Z} \subset \pi^{-1}(\pi(d\mathbb{Z}))$

Montrons l'inclusion inverse. Soit $x \in \pi^{-1}(\pi(d\mathbb{Z}))$,

$\pi(x) \in \pi(d\mathbb{Z}) \Leftrightarrow \exists y \in d\mathbb{Z} \quad \pi(x) = \pi(y)$

$\Leftrightarrow \quad x - y \in \underbrace{n\mathbb{Z}}_{\text{noyau de } \pi} \subset d\mathbb{Z} \Rightarrow x \in d\mathbb{Z}$

Ainsi : $\quad \pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Leftrightarrow d'\mathbb{Z} \supset d\mathbb{Z}$

$\pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Leftrightarrow d' | d$

$\Updownarrow$

$H = G$ ou $\mathbb{Z}/n\mathbb{Z}$

c.à.d :

$\pi(d'\mathbb{Z}) = \pi(d\mathbb{Z})$ ou $\pi(d'\mathbb{Z}) = \pi(\mathbb{Z})$ $\Leftrightarrow \begin{cases} d' = d \\ \text{ou} \\ d' = 1 \end{cases}$

Ainsi $\{G$ maximal ~~d'ordre d~~ $/ \pi(d\mathbb{Z}) = G\} \Leftrightarrow \{\forall d' \; d' | d \Rightarrow d' = d$ ou $d' = 1\}$

$\Uparrow$

d premier

ccl

G maximal $\Leftrightarrow d =$ diviseur premier de n

2-méthode (c'est la mienne !)

Soit $G \subset \mathbb{Z}/n\mathbb{Z}$.

G maximal $\Leftrightarrow \nexists G'$ sous-groupe strict de $\mathbb{Z}/n\mathbb{Z}$ / $G \subsetneq G' \subset \mathbb{Z}/n\mathbb{Z}$

$\Leftrightarrow \nexists\ d' \neq d$ et n tel que $d | d'$ et $d' | n$ $\quad (1)$

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Pro | $G \subset \mathbb{Z}/n\mathbb{Z}$
G maximal, d'ordre $d \iff \exists i \ / \ d = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^{\boxed{\alpha_i - 1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$

($\Leftarrow$) Prenons $d = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Si $d' | n$, alors $d' = p_1^{\beta_1} \cdots p_k^{\beta_k}$ où $\beta_i \leq \alpha_i$ $(\forall i)$

Si $d | d'$, alors $\begin{cases} \alpha_1 - 1 \leq \beta_1 \\ \alpha_i \leq \beta_i & i \in [2, k] \end{cases}$ d'où $\begin{cases} \alpha_1 - 1 \leq \beta_1 \leq \alpha_1 \\ \alpha_i = \beta_i & i \in [2, k] \end{cases}$

c.à.d $d = d'$ ou $n \Rightarrow G$ maximal

($\Rightarrow$) Contraposée.

Si $d = p_1^{\delta_1} \cdots p_k^{\delta_k}$ où $\delta_1 + \cdots + \delta_k \leq (\alpha_1 + \cdots + \alpha_k) - 2$

Alors : $\exists i \in [1, k] \ / \ \delta_i + 1 \leq \alpha_i$

et $d' = p_1^{\delta_1} \cdots p_i^{\delta_i + 1} \cdots p_k^{\delta_k}$ où $\delta_1 + \cdots + (\delta_i + 1) + \cdots + \delta_k \leq (\alpha_1 + \cdots + \alpha_k) - 1$

Alors $d' | n$ et $d | d'$, avec $d' \neq d$ et $d' \neq n$.

$\Downarrow$

G <u>non</u> maximal.

CQFD

3- méthode

préliminaire

Pro | $G \subset \Gamma$ groupe pas forcément commutatif
Alors G sous-groupe maximal $\iff \Gamma / G$ simple

(Def : G est simple ssi G n'admet pas d'autres sous-groupes que $\{\dot{e}\}$ ou G)

Preuve : Par contraposée.

($\Leftarrow$) Supposons G non maximal. Alors : $\exists H \ / \ G \subsetneq H \subsetneq \Gamma$

Soit χ la surjection canonique $\chi : \Gamma \to \Gamma/G$. $\chi(H)$ = sous-groupe de Γ/G.

Alors $* \ \chi(H) \neq \{\dot{e}\}$ sinon ...

$* \ \chi(H) \neq \Gamma/G$ sinon $\forall x \in \Gamma \ \exists y \in H \ / \ \chi(y) = \chi(x)$

$\chi(y x^{-1}) = \dot{e}$

$y x^{-1} \in G \Rightarrow y^{-1} x \in H \Rightarrow \in G$

Mais alors $\Gamma \subset G$, absurde !

($\Rightarrow$) Si Γ/G non simple, $\exists H$ sous-groupe tel que $\{\dot{0}\} \subsetneq H \subsetneq \Gamma/G$

Alors $G \subset \underbrace{\chi^{-1}(H)}_{\text{sous-groupe de } \Gamma} \subset \Gamma$

$\supset$ car χ surjective
$\subset$ toujours

* $\chi^{-1}(H) \neq G$, sinon $\overset{\{\dot{0}\}}{\chi(G)} = \chi(\chi^{-1}(H)) = H$ absurde

* $\chi^{-1}(H) \neq \Gamma$, " $\chi(\Gamma) = H$ absurde.
$\chi(\Gamma) = \Gamma/G$

d'où G non maximal. CQFD

Pro	H simple $\Leftrightarrow H \simeq \mathbb{Z}/p\mathbb{Z}$ où p premier

($\Rightarrow$) Si H est simple, soit $x \in H$ $x \neq e$. Alors $\langle x \rangle = H \Rightarrow H \simeq \mathbb{Z}/p\mathbb{Z}$
et p premier (sinon H non simple)

($\Leftarrow$) Évident.

<u>exercice (suite)</u>

Soit $G \subset \mathbb{Z}/n\mathbb{Z}$. G maximal $\Leftrightarrow (\mathbb{Z}/n\mathbb{Z})/G$ simple

$\Leftrightarrow [\mathbb{Z}/n\mathbb{Z} : G]$ premier

$\Leftrightarrow \dfrac{n}{\text{Card } G}$ premier

G maximal $\Leftrightarrow \# G = d$ et $\dfrac{n}{d}$ premier

Révisions

1°/ $\mathfrak{A}_n$ est engendré par les tricycles

2°/ $\mathfrak{A}_n$ est simple $n \geq 5$

3°/ $\mathfrak{S}_n$ est engendré par $\underbrace{(1,2,\dots,n-1)}_{c}$ et $\underbrace{(n-1,n)}_{t}$

On a $c^k t c^{-k} = (k,n)$ (le faire)

Ainsi $\langle t,c \rangle \supset \{ (r,n) \,/\, r \leq n-1 \}$

On a : $(r,n)(s,n)(r,n) = (r,s)$

donc $\langle t,c \rangle$ contient toutes le transpositions

Valuation :

$$\boxed{v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right)}$$

($k=1$: imp) $\quad$ ($p \in \mathcal{P}$) (en fait somme finie) $\quad \mathbb{Z}$

$$n = \sum_{i=0}^{\infty} a_i p^i \qquad 0 \leq a_i < p$$

(somme finie) Retrouvons la forme du cours :

$$\frac{n}{p^k} = \sum_{i=0}^{\infty} a_i p^{i-k} = \underbrace{\sum_{0 \leq i < k} a_i p^{i-k}}_{A} + \sum_{i \geq k} a_i p^{i-k}$$

$$A = \frac{a_0}{p^k} + \dots + \frac{a_{k-1}}{p} \qquad \text{car } a_i \leq p-1$$

$$\leq (p-1)\left(\frac{1}{p^k} + \dots + \frac{1}{p}\right)$$

$$\leq \frac{p-1}{p} \, \frac{\frac{1}{p^k}-1}{\frac{1}{p}-1} = 1 - \frac{1}{p^k} < 1$$

d'où $E\left(\frac{n}{p^k}\right) = \sum_{i=k}^{\infty} a_i p^{i-k}$ $\quad$ (cf $E(a+\varepsilon) = E(a)$ où $\varepsilon < 1$)

D'où :

$$v_p(n!) = \sum_{k=0}^{\infty} \sum_{i \geq k} a_i p^{i-k}$$ posons ~~$j = k - i - k$~~ $k = i - j$

$$= ~~\sum_{k=0}^{\infty} \sum_{j=0}^{\infty} a_{k+j} p^j = \sum_{j=0}^{\infty} p^j \sum_{k=0}^{\infty} a_{k+j}~~)$$

$$= \sum_{i=0}^{\infty} a_i \sum_{j=0}^{i} p^j = \sum_{i=0}^{\infty} a_i \frac{p^{i+1}-1}{p-1}$$

Pb : Nombre de zéros en base 10 de 100! ?

$$= \max \{ n \,/\, 10^n \mid 100! \}$$

$10^n \mid 100! \iff 2^n$ et 5^n divisent $100! \iff \begin{cases} v_2(100!) \geq n \\ v_5(100!) \geq n \end{cases}$

$$\iff n = \mathrm{Min}(v_2(100!), v_5(100!))$$

Calculons : $v_2(100!) = E\left(\frac{100}{2}\right) + E\left(\frac{100}{4}\right) + E\left(\frac{100}{8}\right) + E\left(\frac{100}{16}\right)$

$$+ E\left(\frac{100}{32}\right) + E\left(\frac{100}{64}\right)$$

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

car $E\left(\frac{x}{2}\right) = E\left(\frac{E(\frac{x}{2})}{2}\right)$

$$v_5(100!) = 24$$

Nombre de zéros en base 12 de 100!

$12^n \mid 100! \iff 2^{2n} \mid 100!$ et $3^n \mid 100!$

$\iff \begin{cases} v_2(100!) \geq 2n \\ v_3(100!) \geq n \end{cases} \iff n = \mathrm{Min}\left(\left[\frac{v_2(100!)}{2}\right], v_3(100!)\right)$

$$n = \mathrm{Min}(48, 48) = 48$$

$$v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right) = \frac{n - \alpha_p(n)}{p-1} \quad (I)$$

$$E\left(\frac{E(x)}{m}\right) = E\left(\frac{x}{m}\right)$$

~~Calcul d~~

Montrer que $\frac{(2a)!\,(2b)!}{a!\,b!\,(a+b)!} \in \mathbb{N}$. (2)

en utilisant la formule (I) : $v_p\left(\frac{C_{2a}^{a} C_{2b}^{b}}{C_{a+b}^{a}}\right) = \frac{1}{p-1}\left[\alpha_p(a+b) + \alpha_p(a) + \alpha_p(b) - \alpha_p(2a) - \alpha_p(2b)\right]$

montrer que c'est ≥ 0

$$\begin{cases} a = \sum a_i p^i \\ b = \sum b_i p^i \end{cases} \quad \begin{cases} 2a = \sum (2a_i) p^i \\ 2b = \sum (2b_i) p^i \end{cases} \quad a+b = \sum (a_i + b_i) p^i$$

en base p

pas forcément en base p !

Il convient de faire très attention.

Cas trivial : $\forall i$, $a_i < \frac{p}{2}$, $b_i < \frac{p}{2}$ (aucune retenue pour $2a$, $2b$, $a+b$)

Alors
$$\alpha_p(a+b) = \alpha_p(a) + \alpha_p(b)$$
$$\alpha_p(2a) = 2\alpha_p(a)$$
$$\alpha_p(2b) = 2\alpha_p(b)$$
et nous avons l'égalité.

Sinon : on l'admettra. Pour donner une démonstration correcte de (2), on utilisera plutôt la formule $v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right)$

$$v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{2a}{p^k}\right) + E\left(\frac{2b}{p^k}\right) - E\left(\frac{a}{p^k}\right) - E\left(\frac{b}{p^k}\right) - E\left(\frac{a+b}{p^k}\right) \geq 0$$

car : $\forall \alpha, \beta \in \mathbb{R}$ $\quad [2\alpha] + [2\beta] - [\alpha] - [\beta] - [\alpha+\beta] \geq 0$

(7)

Aut ~~F~~ $\mathcal{K}$?

$\mathcal{K} = \{e, a, b, c\}$

$f \in \text{Aut}\,\mathcal{K} \Rightarrow f|_{\{a,b,c\}} \in \mathcal{S}\{a,b,c\}$

$$\text{Aut}\,\mathcal{K} \xrightarrow{\Phi} \mathcal{S}\{a,b,c\}$$

Φ est injective (car si f et g coïncident sur $\{a,b,c\}$, elles coïncident ~~en~~ sur $\{1, a, b, c\}$.)

Φ est surjective : soit $\sigma \in \mathcal{S}\{a,b,c\}$, alors ~~$\exists f \in \text{Aut}\,\mathcal{K}$~~ /

$\exists f : \mathcal{K} \to \mathcal{K}$ par $f(~~e~~1) = 1$ et $f(x) = \sigma(x)$ pour $x \in \{a, b, c\}$

f est <u>bijective</u>. Reste à voir que c'est un morphisme.

$$f(xy) = f(x)\, f(y) \ ?$$

Si $x = y$, c'est vrai $\quad f(x^2) = 1 = (f(x))^2$

Si $x = ~~e~~1$, " $\quad f(x) = f(x)$ oui

Si $x \neq y \neq ~~e~~1$ $\left\{ \begin{array}{l} xy = z \quad \text{où } \{x, y, z\} = \{a, b, c\} \\ f(x)f(y) = f(x)f(y) \text{ car } \{f(x), f(y), f(x)\cdot f(y)\} = \{a, b, c\} \end{array} \right.$

d'où

~~$f(xy)$~~ $\{x, y, xy\}$

$\downarrow$

$\{\sigma(x), \sigma(y), \sigma(x)\sigma(y)\}$

<u>Rappel</u> : k = corps commutatif (ce ne sera pas $\mathbb{R}$!)

E = k-espace vectoriel

$f : E \to E$ affine $\Leftrightarrow \exists a \in E \ \exists \ell \in \text{End}(E) \ / \ f = t_a \circ \ell$

$$\forall x \in E \quad f(x) = a + \ell(x)$$

$GA(E) = \{\text{applications affines bijectives}\}$

$GA(E) \overset{\Phi}{\longleftrightarrow} E \times GL(E) \qquad \Phi$ est bijective

$t_a \circ \ell \longleftrightarrow (a, \ell)$

car
$$E \times GL(E) \xrightarrow{\Phi} GA(E)$$
$$(a, \ell) \longmapsto t_a \circ \ell$$

et
$$GA(E) \xrightarrow{\varphi} E \times GL(E)$$
$$f \longmapsto (f(0), t_{-f(0)} \circ \ell)$$

Ainsi $GA(E) \underset{\simeq}{\overset{\Phi}{\rightleftarrows}} E \times GL(E)$

On transporte les structures grace à Φ, sur ~~GA(E)~~ $E \times GL(E)$:

$$(a, \ell) * (a', \ell') = (t_a \circ \ell) \circ (t_{a'} \circ \ell')$$
$$= t_{a + \ell(a')} \circ (\ell \circ \ell')$$

Ainsi : $(a, \ell) * (a', \ell') = (a + \ell(a'), \ell \circ \ell')$

$\neq \underbrace{(a + a', \ell \circ \ell')}_{\text{loi habituelle}}$

On définit sur :

$K \times \operatorname{Aut} K$

une loi "bizarre" grace aux rappels concernant les espaces affines.
On définit la loi . sur $K \times \operatorname{Aut} K$ par :

$$(x, \sigma)(x', \sigma') = (x\, \sigma'(x')), \sigma \circ \sigma')$$

Prenons $k = \mathbb{Z}/2\mathbb{Z}$ $E = K$ (de dimension 2 sur k)
$K = (\mathbb{Z}/2\mathbb{Z})^2$

$GA(K) = \underbrace{\mathcal{S}(K)}_{\text{permutations de } K}$

- $GA(K) \subset \mathcal{S}(K)$ évident
- Inversement ↙

$K = \{0, a, b, c\}$ Soit $\sigma \in \mathcal{S}(K$

(a, b, c) est un repère affine de K puisque : $\{\forall x, y, z$ distincts deux à deux, dans K alors ils sont non colinéaires

Regardons $\sigma(a)$, $\sigma(b)$, $\sigma(c)$

donc $\sigma(a)$, $\sigma(b)$ et $\sigma(c)$ sont distincts 2 à 2

$\exists!\, f \in GA(K)$ telle que $\begin{cases} f(a)=\sigma(a) \\ f(b)=\sigma(b) \\ f(c)=\sigma(c) \end{cases}$ $\Rightarrow$ ~~f(x)=σ~~ f et σ coïncident sur K

Donc $\boxed{GA(K) = \mathcal{S}(K)}$

Que dire de $GL(K)$? $GL(K)$ est l'ensemble des applications affines de K qui laissent 0 invariant. Or $GA(K)=\mathcal{S}(K) \Rightarrow GL(K)$ isomorphe à $\mathcal{S}\{a,b,c\}$ (car a fixé 0), ~~donc~~ c.à.d isomorphe à $\mathrm{Aut}\, K$

~~d'où $\mathcal{S}_4 \simeq K \times \mathcal{S}_3$~~

$$\underbrace{GA(K)}_{\mathcal{S}(K) \simeq \mathcal{S}_4} \simeq K \times \overbrace{GL(K)}^{\text{on a vu que c'est isomorphe à } \mathcal{S}_{\{a,b,c\}} = \mathcal{S}_3}$$

produit bizarre !

d'où $\boxed{\mathcal{S}_4 \simeq K \times \mathcal{S}_3}$

↑ produit bizarre.

(14)

a est un carré $\Leftrightarrow$ $a = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ $p_1, \cdots, p_k$ = nombres premiers.

Montrons que a est un carré $\Leftrightarrow$ le nbre de diviseurs de a est impair

($\Rightarrow$) a possède $(2\alpha_1+1)\cdots(2\alpha_k+1)$ = un nbre impair de diviseurs.

($\Leftarrow$) Soit $a = p_1^{\beta_1} \cdots p_k^{\beta_k}$ et $(\beta_1+1)\cdots(\beta_k+1)$ impair $\Rightarrow$ β_i+1 impair
$\Rightarrow$ β_i pair.

CQFD

(10)

lemme : $\forall a, b \in \mathbb{Z}$ $\forall p \in \mathcal{P}$ $v_p(a+b) \geq \mathrm{Min}(v_p(a), v_p(b))$ (L)

En effet : $\begin{cases} a = p^\alpha a' & \delta(a', p) = 1 \\ b = p^\beta b' & \delta(b', p) = 1 \end{cases}$ $\Rightarrow$ $a+b = p^\alpha(a' + p^{\beta-\alpha} b')$ si $\alpha \leq \beta$

donc $v_p(a+b) \geq \mathrm{Min}(v_p(a), v_p(b))$

Soit $a_i \in \mathbb{Z}$, $\sum_{i=1}^{n} a_i = 0$. $\forall p \in \mathcal{P}$, $\mathrm{Min}\{v_p(a_i) / 1 \leq i \leq n\}$ est atteint au moins 2 fois.

Supposons que $\mathrm{Min}_{i \in [1,n]}(v_p(a_i)) = v_p(a_1)$.

Alors $\sum_{i=2}^{n} a_i = -a_1$ (1)

et $v_p\left(\sum_{i=2}^{n} a_i\right) \geq \mathrm{Min}_{i \in [2,n]}(v_p(a_i))$. (voir lemme) (2)

Si $\mathrm{Min}_{i \in [2,n]}(v_p(a_i)) \neq v_p(a_1)$, alors $v_p\left(\sum_{i=2}^{n} a_i\right) > v_p(a_1)$ ce qui est absurde eu égard à (1)

Le minimum des valuations p-adiques est atteint au moins 2 fois. CQFD

on aurait pu faire un raisonnement direct :

(1) et (2) $\Rightarrow$ $v_p(a_1) \geq \mathrm{Min}_{i \in [2,n]}(v_p(a_i))$
$\Downarrow$
$\exists k \in [2,n]$ / $v_p(a_1) = v_p(a_k)$

Généralisation de cette propriété

On sait définir la valuation p-adique d'un nombre rationnel :

$\forall m = \frac{p_0}{q_0} \in \mathbb{Q}$ $v_p(m) = v_p(p_0) - v_p(q_0)$

En faisant la m̂ démonstration que ci-dessus, on constate que, si $\sum_{i=1}^{n} a_i = 0$

où $a_i \in \mathbb{Q}$, alors $\underset{i\in[1,n]}{\mathrm{Min}}(v_p(a_i))$ est atteint au moins 2 fois.

Notons (P) cette propriété.

Montrer que $S_n = 1 + \dots + \frac{1}{n}$ $(n \geqslant 2)$ n'est jamais entier

~~Supposons, par l'absurde, que $S_n \in \mathbb{N} \subset \mathbb{Q}$. Alors~~ :

- $S_n \in \mathbb{Q}$ $\qquad 1 + \dots + \frac{1}{n} - S_n = 0$

D'après la propriété (P) ; $\underset{x\in[1,n]}{\mathrm{Min}}\left(v_2\left(\frac{1}{x}\right), v_2(S_n)\right)$ est atteint au moins 2 fois.

- Si nous montrons que $\underset{x\in[1,n]}{\mathrm{Min}}\left(v_2\left(\frac{1}{x}\right)\right)$ est atteint seulement en une valeur de x, et que cette valeur est négative, alors on aura montré que $v_2(S_n) = \underset{x\in[1,n]}{\mathrm{Min}}\left(v_2\left(\frac{1}{x}\right)\right) < 0$

c.à.d : $S_n \notin \mathbb{N}$.

Preuve :

- Comme $v_2\left(\frac{1}{2}\right) = -1$, $\underset{x\in[1,n]}{\mathrm{Min}}\left(v_2\left(\frac{1}{x}\right)\right) < 0$

Comme $v_2\left(\frac{1}{x}\right) = -v_2(x)$, il suffit de montrer que « $v_2(x)$ atteint une fois son maximum pour $x = 1, \dots, n$ ». Pour cela, on observera que :

$v_2(1) = 0$
$v_2(2) = 1$
$v_2(3) = 0$
$v_2(4) = 2$ ← $4 = 2^2$ maximum unique.
$v_2(5) = 0$
$v_2(6) = 1$

NB : Ça ne marche pas pour $p \in \mathcal{P}$, $p \neq 2$ car, au lieu d'être atteint seulement en 2^α, il le sera peut-être en tous les nombres de la forme $p^\alpha, 2p^\alpha, \dots, (p-1)p^\alpha$

$\forall n \in \mathbb{N}$ $(n \geqslant 2)$ $\qquad \exists \alpha \in \mathbb{N} \ / \ 2^\alpha \leqslant n < 2^{\alpha+1}$

Alors $\boxed{\begin{matrix}\forall x \in [1,n] \\ x \neq 2^\alpha\end{matrix} \Rightarrow v_2(x) < \underbrace{v_2(2^\alpha)}_{=\alpha}}$.

En effet : par l'absurde (↑ en fait, la contraposée). Si $v_2(x) = \alpha' \geqslant \alpha$, alors $x = 2^{\alpha'}q$ $\alpha' \geqslant \alpha$ et $\Delta(q,2) = 1$

$\begin{cases} \text{Si } q=1 & x = 2^{\alpha'} \text{. Mais alors } \alpha' \geq \alpha \text{ et } x \neq 2^{\alpha} \Rightarrow x \notin [1,n] \text{, absurde.} \\ \text{Si } q \neq 1 & , q > 2 \Rightarrow x = 2^{\alpha'} q > 2^{\alpha+1} \Rightarrow x \notin [1,n] \text{ absurde.} \end{cases}$

CQFD

(14) $a \in \mathbb{N}$

$\mathcal{D}(a) = \{d \,/\, d \text{ divise } a\}$

$\#\mathcal{D}(a) \text{ impair} \Leftrightarrow \exists b \in \mathbb{N} \,/\, a = b^2$

$\mathcal{D} = \mathcal{D}' \cup \mathcal{D}''$

$\begin{cases} \mathcal{D}' = \{d \,/\, d \leq \frac{a}{d}\} \\ \mathcal{D}'' = \{d \,/\, d \geq \frac{a}{d}\} \end{cases}$ (et $d | a$, évidemment)

On remarque que : $f : \mathcal{D}' \to \mathcal{D}''$, $d \mapsto \frac{a}{d}$ bijective. (f involutive)

donc $\#\mathcal{D}' = \#\mathcal{D}'' = n$

$\# \mathcal{D} = 2n - \#(\underbrace{\mathcal{D}' \cap \mathcal{D}''})$

$\parallel$

$\emptyset$ ou contient un seul élément $d \,/\, d^2 = a$.

D'où

~~# D pair~~

$\begin{cases} \#(\mathcal{D}' \cap \mathcal{D}'') = 0 \Leftrightarrow a \neq \text{carré} \Leftrightarrow \#\mathcal{D} \text{ pair} \\ \#(\mathcal{D}' \cap \mathcal{D}'') = 1 \Leftrightarrow a = \text{carré} \Leftrightarrow \#\mathcal{D} \text{ impair} \end{cases}$

(8) $Aut(\mathbb{Z}/n\mathbb{Z})$?

On considère $\begin{array}{ccc} Aut(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ f & \longmapsto & f(\dot{1}) = \dot{a} \end{array}$ (1)

Si $f \in Aut(\mathbb{Z}/n\mathbb{Z})$, $f(\dot{1})$ = élément d'ordre n (car f conserve l'ordre.)

Il y a $\varphi(n)$ él. d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$

$f(\dot{1}) = \dot{a}$ $\quad a \in \mathbb{Z}$ et $\delta(a,n) = 1$

Inversement, si $f(\dot{1}) = a$ $\quad \delta(a,n) = 1$, alors f, automorphisme, est parfaitement déterminé.

$\# Aut(\mathbb{Z}/n\mathbb{Z}) = \varphi(n)$

Et la structure de groupe de $(Aut(\mathbb{Z}/n\mathbb{Z}), \circ)$?

$$f \circ g(\dot{1}) = f(g(\dot{1})) = f(b.\dot{1}) = b\, f(\dot{1}) = b\dot{a} = \widehat{ba}$$

donc $(Aut(\mathbb{Z}/n\mathbb{Z}), \circ)$ est commutatif, ce qui ne sautait pas aux yeux

De plus : $f \circ g(\dot{1}) = \widehat{ba} = \dot{b}\dot{a} = \dot{f(\dot{1})} \times \dot{g(\dot{1})}$ (2)

Remarque : A anneau $\quad \mathcal{U}(A) = \{x \in A \,/\, \exists x' \;\; xx' = 1\}$

$\mathcal{U}(A)$ est un groupe pour $\times$

Par exemple $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$

$\mathcal{U}(K) = K^*$ (si K = corps)

On a donc montré en (1) et (2), que $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

(9) $N(a,b) = \dfrac{(2a)!\,(2b)!}{a!\,b!\,(a+b)!}$

On sait que
$$\boxed{v_p(x!) = \sum_{k=1}^{\infty} E\left(\frac{x}{p^k}\right)}$$

Preuve de la formule :

Si $x < p$, la formule est vraie.

Si $x \geq p$, on écrit : $x! = \underbrace{1.2.3.\cdots}_{} p \underbrace{\cdots}_{} 2p \underbrace{\cdots}_{} ap \underbrace{\cdots}_{} x$ ~~(a+1)p~~

↑ pas de facteur p dans la déc. en n.p. ↑ pas de facteur p (d.n.p.)

$$\nu_p(x!) = \nu_p(p^a a!)$$

et $a = E\left(\frac{x}{p}\right)$

Donc $\nu_p(x!) = E\left(\frac{x}{p}\right) + \nu_p\left(E\left(\frac{x}{p}\right)!\right)$

Et, on recommence :

$$\nu_p(x!) = E\left(\frac{x}{p}\right) + E\left(\frac{E\left(\frac{x}{p}\right)}{p}\right) + \nu_p\left(E\left(\frac{E\left(\frac{x}{p}\right)}{p}\right)!\right) \quad (1)$$

Lemme : $\left[\frac{[y]}{p}\right] = \left[\frac{y}{p}\right]$

$y = [y] + a \qquad a < 1$

$[y] = pq + r \qquad r \leq p-1$

$\frac{[y]}{p} = q + \frac{r}{p} \qquad \left[\frac{[y]}{p}\right] = q$

$\frac{y}{p} = \frac{[y]+a}{p} = q + \frac{r+a}{p}$ et $r + a < p \Rightarrow \frac{r+a}{p} < 1$

donc $\left[\frac{y}{p}\right] = q$ CQFD

(1) donne $\nu_p(x!) = \left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \cdots + \left[\frac{x}{p^k}\right]$

Retour à l'exercice :

$$\nu_p(N(a,b)) = \nu_p(2a!) + \nu_p(2b!) - \nu_p(a!) - \nu_p(b!) - \nu_p((a+b)!)$$

$$= \sum_{k=1}^{\infty} \left[\frac{2a}{p^k}\right] + \left[\frac{2b}{p^k}\right] - \left[\frac{a}{p^k}\right] - \left[\frac{b}{p^k}\right] - \left[\frac{a+b}{p^k}\right]$$

• Montrons que :

$\forall x, y \in \mathbb{R} \quad [2x] + [2y] - [x] - [y] - [x+y] \geq 0$

Preuve :

Envisager les cas $\begin{cases} x = [x] + a & a < 1 \\ y = [y] + b & b < 1 \end{cases}$

① $a < \frac{1}{2}$ et $b < \frac{1}{2}$

② $a < \frac{1}{2}$ et $b \geq \frac{1}{2}$

③ $a \geq \frac{1}{2}$ et $b \geq \frac{1}{2}$

On calcul l'expression dans chacun de ces cas. On trouve chaque fois 1 ou 0.

2- méthode

$N(a+1, b) + N(a, b+1) = 4\, N(a, b)$

Par récurrence $\quad N(a, b+1) = \underbrace{4\, N(a, b)}_{\in \mathbb{N}} - \underbrace{N(a+1, b)}_{\in \mathbb{N}}$

(13) Prendre $H = \mathbb{Z}$

$H' = n\mathbb{Z} \quad (n \neq 1,\ n \neq 0)$

et $\mathbb{Z} \longrightarrow n\mathbb{Z}$

$x \longmapsto nx$ est une isomorphisme de groupes.

et pourtant $\mathbb{Z}/n\mathbb{Z} \not\cong \underbrace{\mathbb{Z}/\mathbb{Z}}_{= \{0\}}$

UNIVERSITÉ DE NICE
INSTITUT DE MATHÉMATIQUES ET SCIENCES PHYSIQUES
PARC VALROSE
06034 NICE CEDEX
TÉL. (93) 51.91.00
MATHÉMATIQUES

M1 Algèbre et Arithmétique.

Feuille N°4.

× 1°) Montrer que pour qu'un produit de groupes soit cyclique, il faut et il suffit qu'ils le soient tous deux, et que leurs cardinaux soient premiers entre eux.

× 2°) Résoudre les systèmes de congruences : $\begin{cases} x \equiv 3 \ (4) \\ x \equiv 0 \ (3) \end{cases}$ (fait au tableau.)

$\begin{cases} x \equiv 2 \ (6) \\ x \equiv 5 \ (9) \end{cases}$ $\begin{cases} x \equiv 15 \ (32) \\ x \equiv 7 \ (26) \end{cases}$

× 3°) (Pb du cuisinier chinois) Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident qu'une fois arrivés à terre ils partageront également les pièces d'or entre eux, et donneront le reste, soit trois pièces d'or au cuisinier chinois. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés et le partage laisserait 5 pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

9.01.78

4° Soit H un sous-groupe de $(\mathbb{Z}^2, +)$ qu'on suppose non réduit à $\{(0,0)\}$.

A) On suppose que pour tout couple $((a,b),(c,d))$ d'éléments de H on a $ad-bc=0$.

α) S'il existe un élément $(0,b) \neq 0$ dans H, alors tout élément de H est de cette forme et H est engendré par un élément ; même résultat pour $(a,0) \neq 0$ dans H.

β) Sinon, soit $(a,b) \in H$, avec $d = \text{pgcd}(a,b)$ et $d = \min\{\text{pgcd}(x,y) \mid (x,y) \in H, x \neq 0, y \neq 0\}$ (on prend les pgcd > 0)

alors, (a,b) engendre H.

B) On suppose maintenant qu'il existe des couples $((a,b),(c,d))$ dans $H \times H$ vérifiant $ad-bc \neq 0$, et soit un tel couple vérifiant en outre $\delta = ad-bc = \inf\left\{vx-uy \,\middle|\, \begin{matrix}(x,y) \in H \\ (u,v) \in H\end{matrix}, vx-uy>0\right\}$

α) On considère les applications φ et ψ de H dans $\mathbb{Z}$ définies par $\varphi(x,y) = ay - bx$ et $\psi(x,y) = cy - dx$. Montrer que $\varphi(H)$ et $\psi(H)$ sont des sous-groupes de $\mathbb{Z}$.

β) En déduire $\varphi(H) = \psi(H) = \delta\mathbb{Z}$.

γ) Montrer que $\{(a,b),(c,d)\}$ engendre H.

[Si $(x,y) \in H$, $\delta \mid \varphi(x,y)$ et $\delta \mid \psi(x,y)$].

Suite Feuille 4
M1. Alg. Arith.
9.01.78

1^re méthode : A montrer :

① $G_1 \times G_2$ cyclique $\Leftrightarrow$ G_1 et G_2 cycliques et $\delta(n_1, n_2) = 1$

($\Leftarrow$) [G cyclique $\Leftrightarrow$ $\forall d$ $d | n$ $\#\{x \in G / dx = 0\} \leq d$] (rappel de cours)

d / $d | n$ et $n = n_1 n_2$

On va essayer d'écrire $d = d_1 d_2$ où $d_1 | n_1$ et $d_2 | n_2$.

(Ce ~~n'~~est ~~pas~~ toujours le cas ↓ ~~$n_1 = 4$ $n_2 = 6$~~)

Soit $d | n_1 n_2$ $\quad d_1 = \text{pgcd}(d, n_1)$ $\Rightarrow \begin{cases} d = d_1 d_2 \\ n_1 = d_1 n_1' \end{cases}$ et $\delta(d_2, n_1') = 1$

$d_1 d_2 | n_1 n_2 \Rightarrow d_2 | n_2 n_1' \Rightarrow d_2 | n_2$ (gauss) d'où $n_2 = d_2 n_2'$

donc $d = d_1 d_2$ où $d_1 | n_1$ et $d_2 | n_2$

Montrons que cette décomposition $d = d_1 d_2$ est unique, si $(n_1, n_2) = 1$:

Si $\delta(n_1, n_2) = 1$ $\quad d_1 d_2 = d_1' d_2' = d$ divise n $\Rightarrow d_1 = d_1'$, $d_2 = d_2'$

En effet $\left.\begin{array}{c} d_1 | d_1' d_2' \\ \text{et} \\ \delta(d_1, d_2') = 1 \end{array}\right\} \Rightarrow d_1 | d_1'$ de même $d_1' | d_1 \Rightarrow d_1 = d_1'$

Conclusion :

Retour à l'exercice :

$d_1 | n_1$, $\# \overbrace{\{x_1 \in G_1 / d_1 x_1 = 0\}}^{E_1} \leq d_1$

$d_2 | n_2$, $\# \underbrace{\{x_2 \in G_2 / d_2 x_2 = 0\}}_{E_2} \leq d_2$

On cherche l'ensemble des couples (x_1, x_2) tels que $d.(x_1,x_2)=0$.

$$d(x_1,x_2)=0 \Leftrightarrow \begin{cases} d_1 d_2 x_1 = 0 \\ d_1 d_2 x_2 = 0 \end{cases} \underset{(*)}{\Leftrightarrow} \begin{cases} d_1 x_1 = 0 \\ d_2 x_2 = 0 \end{cases}$$

(*)
En effet :

$d_1 x_1 \in G_1$ $\quad d_2(d_1 x_1) = 0 \Leftrightarrow \underbrace{\omega(d_1 x_1)}\ |\ d_2$

c'est un diviseur de n_1
et aussi diviseur de n_2 car $d_2 | n_2$. $\Rightarrow \omega(d_1 x_1) = 1$
Donc $d_1 x_1 = 0$

Donc $E = \{(x_1,x_2) / d(x_1,x_2)=0\} = E_1 \times E_2$ ⚡

$$\Downarrow$$

$$\text{Card } E \leq d_1 \times d_2 = d$$

($\Rightarrow$) Inversement, supposons que $\text{Card } E \leq d$.

- $d_1 | n_1$, $\# \underbrace{\{x_1 \in G_1 / d_1 x_1 = 0\}}_{E_1} \overset{?}{\leq} d_1$

$d_1 | n_1 \Rightarrow d_1 | n$ et $\# \{x \in G / d_1 x = 0\} \leq d_1$

$$x_1 \in E_1 \hookrightarrow (x_1, 0) \in E$$

donc $\text{Card } E_1 \leq \text{Card } E \leq d_1$

- ~~Es $\delta(n_1,n_2)$~~ Soit $= d$ un diviseur commun à n_1 et à n_2

$d | n_1$ et $d | n_2 \Rightarrow d | n$

On sait que $\# \{x \in G / \underset{0}{\underset{\shortparallel}{dx}}\} = d$

Or $\{x \in G / dx = 0\} = \{x_1 \in G_1 / dx_1 = 0\} \times \{x_2 \in G_2 / dx_2 = 0\}$

$$\Downarrow$$

$$d^2 = d$$

$$\Downarrow$$

$$d = 1$$

<u>2e méthode</u> : A montrer : $G = G_1 \times G_2$ cyclique $\Leftrightarrow$ G_1 et G_2 cycliques et $\delta(n_1, n_2) = 1$

($\Leftarrow$) $G_1 = \langle h \rangle$, $G_2 = \langle k \rangle$

Alors $\omega(h,k) = \text{ppcm}(\omega(h), \omega(k)) = n_1 n_2 \Rightarrow (h,k)$ engendre G.
(cf. lemme)

($\Rightarrow$) Si $\underbrace{\omega(h,k)}_{\text{ppcm}(\omega(h),\omega(k))} = n_1 n_2$

Posons $\begin{cases} n_1 = \omega(h)\, n'_1 \\ n_2 = \omega(k)\, n'_2 \end{cases}$. Alors on obtient : $\text{ppcm}(\omega(h), \omega(k)) = \omega(h)\omega(k)\, n'_1 n'_2$

$$1 = n'_1 n'_2\, \delta(\omega(h), \omega(k))$$
$$\Updownarrow$$
$$n'_1 = n'_2 = \delta(\omega(h), \omega(k)) = 1$$

D'où $\begin{cases} \omega(h) = n_1 \\ \omega(k) = n_2 \end{cases}$ et $\delta(n_1, n_2) = 1$. CQFD

<u>lemme</u> $\boxed{\omega(h,k) = \text{ppcm}(\omega(h), \omega(k))}$

En effet $n(h,k) = (0,0) \Leftrightarrow \begin{cases} nh = 0 \Rightarrow \omega(h) \mid n \\ nk = 0 \Rightarrow \omega(k) \mid n \end{cases} \Rightarrow \text{ppcm}(\omega(h), \omega(k)) \mid n$

et $\text{ppcm}(\omega(h), \omega(k))\, (h,k) = (0,0)$, donc $\omega(h,k) = \text{ppcm}(\omega(h), \omega(k))$.
(oui)

<u>Remarque</u> :

Cet exercice contient le théorème chinois.

$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique, isomorphe à $\mathbb{Z}/ab\mathbb{Z}$, ssi $\delta(a,b) = 1$

③ n pièces d'or

a) 17 pirates $n \equiv 3 \ [17]$ } (1)

b) 11 pirates $n \equiv 4 \ [11]$

c) 6 pirates $n \equiv 5 \ [6]$

(1) $\Delta(11,17) = 1$ ~~divise 4-3~~ $\Rightarrow \exists$ solution unique modulo $ppcm(17,11) = 17 \times 11 = 187$

$n = 3 + 17\ell$

$3 + 6\ell \equiv 4 \ [11]$

$6\ell \equiv 1 \ [11]$ et $\dot{6} . \dot{2} = \dot{1}$ dans $\mathbb{Z}/11\mathbb{Z}$

$\Updownarrow$

$\ell \equiv 2 \ [11]$

$\ell = 2 + 11u$ d'où $n = 37 + 187u$ $u \in \mathbb{Z}$

(2) $\begin{cases} n \equiv 37 & [187] \\ n \equiv 5 & [6] \end{cases}$

$\Delta(187,6) \Rightarrow \exists !$ solution modulo $187 \times 6 = 1122$

On a $187\ell + 37 \equiv 5 \ [6]$

$187\ell \equiv 4 \ [6]$

$\ell \equiv 4 \ [6]$

d'où $n = 1122u + 785$. Le plus petit gain possible est donc 785 pièces

Rappel : Suite Exacte

$$0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \longrightarrow 0$$

Exercice (4)

- Soit H un sous-groupe de $(\mathbb{Z}^2,+)$, $H \neq \{(0,0)\}$

A) Si $\forall((a,b),(c,d)) \in H^2$ on a $ad-bc=0$

α) S'il existe un élément $(0,b) \neq (0,0)$ dans H, alors tout élément de H est de cette forme et H est engendré par un élément $(0,b)$.
Même résultat pour $(a,0) \in H$.

β) Sinon, soit $(a,b) \in H$ avec $d = \Delta(a,b) = \mathrm{Min}\{\delta(x,y) \,/ (x,y) \in H \;\; x \neq 0, y \neq 0\}$ (on prend les pgcd >0). Alors (a,b) engendre H.

- B) Si $\exists ((a,b)(c,d)) \in H^2$ tels que $ad-bc \neq 0$. Soit un tel couple vérifiant, en outre $\delta = ad-bc = \mathrm{Inf}\left\{vx-uy \,/ \begin{matrix}(x,y)\in H \\ (u,v)\in H\end{matrix} \text{ et } vx-uy>0\right\}$

α) On considère les applications φ et ψ de H dans $\mathbb{Z}$ définies par $\varphi(x,y) = ay - bx$ et $\psi(x,y) = cy - dx$. Montrer que $\varphi(H)$ et $\psi(H)$ sont des sous-groupes de $\mathbb{Z}$

β) En déduire $\varphi(H) = \psi(H) = \delta\mathbb{Z}$

γ) Montrer que $((a,b),(c,d))$ engendre H et que $H \simeq \mathbb{Z}^2$

[Indications : Si $(x,y) \in H$ $\quad \delta \mid \varphi(x,y)$ et $\delta \mid \psi(x,y)$]

-

Solution

A) α) $\forall (a_1,a_2) \in H \qquad a_1 b - a_2 0 = 0 \Rightarrow a_1 = 0$ oui

Soit $f : \mathbb{Z} \to f(\mathbb{Z})$ est un isomorphisme
$b \mapsto (0,b)$

$H \subset f(\mathbb{Z}) \qquad f^{-1}(H) = \text{sous-groupe de } \mathbb{Z} = n\mathbb{Z}$ et $f(f^{-1}(H)) = H$ car $H \subset \mathrm{Im} f$

engendré par n

d'où $H = f(n\mathbb{Z}) \Rightarrow H$ engendré par $f(n) = (0,n)$

β) $(x,y),(a,b) \in H \Rightarrow xb - ay = 0 \Rightarrow xb = ya$

$d = \Delta(a,b)$, $a = da'$, $b = db'$ d'où $xb' = ya'$ (1)

$a' | xb'$ et $\Delta(a',b') = 1 \Rightarrow a' | x \Rightarrow \exists n_1 \in \mathbb{Z} \,/\, x = n_1 a'$

Alors (1) : $y = n_1 b'$

Ainsi : $\begin{cases} x = n_1 a' \\ y = n_1 b' \end{cases}$ (2)

Comme $\delta = \Delta(x,y) = \Delta(n_1 a', n_1 b') = n_1 \geq d$, on peut faire la division euclidienne de n_1 par d :

$n_1 = dq + r$ où $0 \leq r < d$

Alors $\begin{cases} x = dqa' + ra' = qa + ra' \\ y = dqb' + rb' = qb + rb' \end{cases} \Rightarrow \underbrace{(x,y)}_{\in H} = \underbrace{q(a,b)}_{\in H} + r(a',b')$

donc $r(a',b') \in H$, mais $\Delta(a',b') = 1 \Rightarrow \delta(ra', rb') = r < d$! absurde.

Donc $r = 0$, autrement dit : $n_1 = dq$.

(2) $\Rightarrow \begin{cases} x = qa \\ y = qb \end{cases}$

On a montré que $(x,y) \in H \Rightarrow \exists q \in \mathbb{Z}$ $(x,y) = q(a,b)$, ce qui prouve que $H = \langle (a,b) \rangle$.

CQFD

B) α) $\varphi, \psi : H \to \mathbb{Z}$ sont des morphismes de groupe.

donc $\varphi(H)$ et $\psi(H)$ = sous-groupes de $\mathbb{Z}$.

β) Posons $\varphi(H) = \ell\mathbb{Z}$ $(\ell > 0)$

- $\varphi(c,d) = ad - bc = \delta \Rightarrow \delta\mathbb{Z} \subset \ell\mathbb{Z} \Rightarrow \ell \leq \delta$
- $\exists (x,y) \in H \,/\, \varphi(x,y) = ay - bx = \ell > 0 \Rightarrow \delta \leq ay - bx = \ell \Rightarrow \delta \leq \ell$

$\Big\}\ \delta = \ell$

Ainsi

$\boxed{\varphi(H) = \delta\mathbb{Z}}$

(On remarque que tout marche bien parceque les bornes sont atteintes)

(m̂ chose avec ψ)

γ) On doit montrer que

$\forall (x,y) \in H \quad \exists\, n,m \ / \quad (x,y) = n(a,b) + m(c,d)$

$$(x,y) = (na + mc,\ nb + md)$$

$$\begin{cases} x = na + mc \\ y = nb + md \end{cases}$$

d'où :

$$\begin{cases} n = \dfrac{\begin{vmatrix} x & c \\ y & d \end{vmatrix}}{ad-bc} = \dfrac{dx-cy}{\delta} \in \mathbb{Z} \quad (\text{car } \delta \mid dx-cy) \\[2ex] m = \dfrac{\begin{vmatrix} a & x \\ b & y \end{vmatrix}}{ad-bc} = \dfrac{ay-bx}{\delta} \in \mathbb{Z} \quad (\text{car } \delta \mid ay-bx) \end{cases}$$

CQFD.

On a $\quad \Phi : \mathbb{Z}^2 \longrightarrow H$

$\qquad (n,m) \longmapsto n(a,b) + m(c,d) \quad$ (Φ est un isomorphisme de groupes)

(Remarque : interprétation géométrique, $\det\left[\binom{a}{b}\binom{c}{d}\right]$ = aire du parallélogramme construit sur $\binom{a}{b}\binom{c}{d}$)

Exercice

- Soit G un groupe. $D(G)$ = groupe dérivée ≑ plus petit sous-groupe de G contenant tous les éléments de la forme $xyx^{-1}y^{-1}$ $(x,y \in G)$.

Montrer que, si u = endomorphisme de G, alors

1°/ $u(D(G)) \subset D(G)$

2°/ si $H \triangleleft G$, $\quad G/_H$ abélien $\Leftrightarrow D(G) \subset H$

1°/

$$D(G) = \{ z \in G \ / \quad z = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \quad a_i = x_i y_i x_i^{-1} y_i^{-1} \text{ et } \varepsilon_i = \pm 1 \}$$

$$u(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}) = u(a_1)^{\varepsilon_1} \cdots u(a_n)^{\varepsilon_n}$$

et $\quad u(a_i) = u(x_i)u(y_i)\,u(x_i)^{-1}\,u(y_i)^{-1} \in D(G)$

d'où $\quad u(D(G)) \subset D(G)$

2°/ $\quad G/H$ abélien $\Leftrightarrow \forall x,y \in G \quad$ ~~$xH \times yH = (xy)H = (yx)$~~

$\qquad Hx \times Hy = H(xy) = H(yx)$

$\Leftrightarrow \quad xy(yx)^{-1} \in H$

$\Leftrightarrow \forall x,y \in G \quad xyx^{-1}y \in H \Leftrightarrow \quad D(G) \subset H$

CQFD

Extension

Soit G un groupe. Les éléments embêtants sont ceux qui ne commutent pas avec les autres. On les réunit en un sous-groupe ("on les met dans le même sac") puis on fait le quotient de G par D(G) qui est distingué.
(voir D(G) invariant par tout automorphisme intérieur de G, cf d°/)
L'embêtement a disparu : le groupe quotient est commutatif.

$$\underset{\text{non abélien}}{G} \xrightarrow{\pi} \underset{\text{abélien}}{G/D(G)}$$

TD ALG [5]

UNIVERSITÉ DE NICE

INSTITUT DE MATHÉMATIQUES
ET SCIENCES PHYSIQUES

PARC VALROSE
06034 NICE CEDEX
TÉL. (93) 84.60.29

MATHÉMATIQUES

M1 Algèbre et Arithmétique
78-79
le 24.01.79

Feuille N° 5

1° Résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} 4x + y + z - t = 6 \\ x + y + 3z + 2t = -3 \\ 2x - 3y + 2z - 3t = 3 \end{cases}$$

2° Trouver toutes les matrices à coefficients entiers de la forme $\begin{pmatrix} 1 & 4 & * \\ 2 & 5 & * \\ 1 & 6 & * \end{pmatrix}$ et de déterminant 1

3° Trouver les matrices diagonales équivalentes aux matrices suivantes :

$$\begin{pmatrix} 0 & 2 & 4 & -1 \\ 6 & 12 & 14 & 5 \\ 0 & 4 & 14 & -1 \\ 10 & 6 & -4 & 11 \end{pmatrix} \quad \begin{pmatrix} 0 & 6 & -9 & -3 \\ 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 66 & 78 & 81 & 63 \end{pmatrix} \quad \text{etc...}$$

4° On considère le morphisme $f : \mathbb{Z}^3 \to \mathbb{Z}^4$ dont la matrice, dans les bases canoniques est $\begin{pmatrix} 2 & 0 & 1 \\ -1 & 2 & 4 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix}$

Identifier Ker f et Im f (Trouver leur rang) et calculer le conoyau de f.

× 5°) Soit G le groupe additif des polynômes à coefficients entiers de degré ≤ 4. Montrer que le quotient de G par le sous-groupe engendré par les polynômes $8X+21$, $4X+9$, $5X^2$, $7X^3+7X^4$ est $\simeq \mathbb{Z}/420\mathbb{Z} \times \mathbb{Z}$

× 6°) Soit $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ de matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; donner une CNS sur a, b, c, d pour que $\mathbb{Z}^2/\mathrm{Im} f$ soit cyclique. préciser la structure de $\mathbb{Z}^2/\mathrm{Im} f$ si f a pour matrice $\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$. (Partiel 78)

× 7°) Trouver un générateur de $U(\mathbb{Z}/17\mathbb{Z})$; combien y en a-t-il ?

× 8°) Déterminer les nombres n pour lesquels $U(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

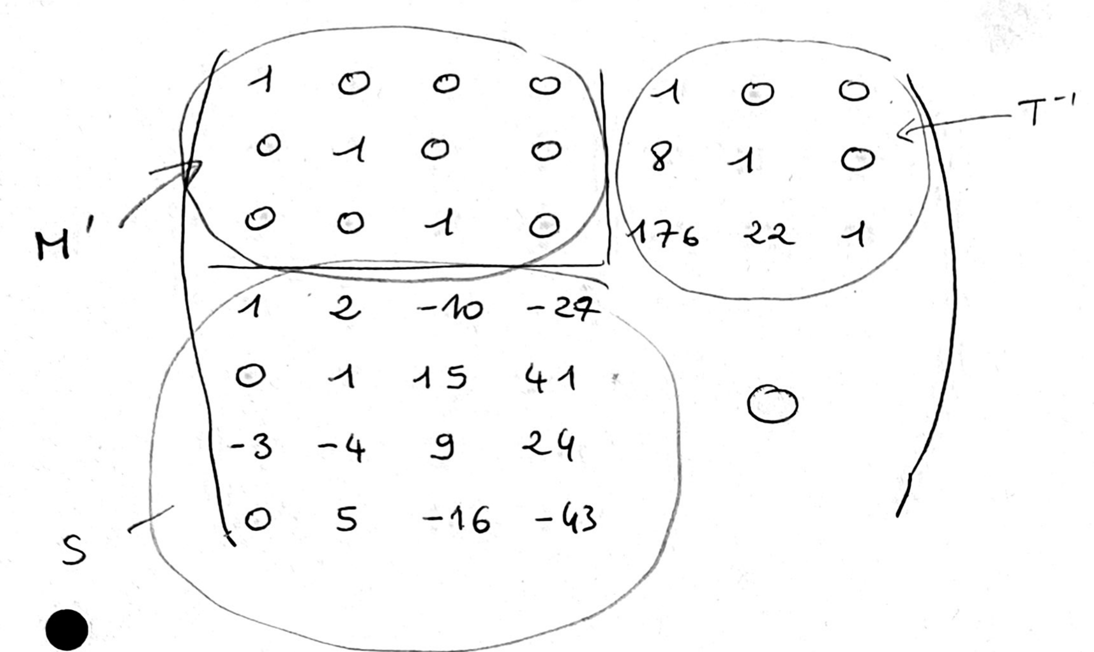
AR

× 9°) Montrer que l'équation $(n^2+1)x - (n+1)y = 1$ n'est résoluble dans $\mathbb{Z}$ que si n est pair. Quelles sont ses solutions ?

× 10°) Montrer que pour tout entier n, 2730 divise $n^{13} - n$.

M 1 Alg. Arith.
F.S. Srita
24.09.79

(1) on trouve, après réductions par opérations élémentaires



-

$X \; \mathcal{B} \xrightarrow{M} \mathcal{F}$

$S \uparrow$ $\mathcal{B}'$ X' ; $T \uparrow$ $\mathcal{F}'$ Y'

$M' = T^{-1}MS$ est donné dans la matrice.

- Y donné $Y' = T^{-1}Y$ — T^{-1} lu sur la matrice

  X cherché $X = SX'$ — S

d'où $Y' = \begin{pmatrix} 6 \\ 45 \\ 993 \end{pmatrix}$

et

$$\left\{ \begin{array}{l} X' = \begin{pmatrix} 6 \\ 45 \\ 993 \\ t \end{pmatrix} \\ \forall t \in \mathbb{R} \end{array} \right. \Rightarrow X = SX' = \begin{pmatrix} -9834 - 27u \\ 14945 + 41u \\ 8739 + 24u \\ -15713 - 43u \end{pmatrix}$$

On peut simplifier ce résultat en posant $v = -364 - u$.

on trouve :

$$x = \begin{pmatrix} -6 + 27v \\ 21 - 41v \\ 3 - 24v \\ -61 + 43v \end{pmatrix} \quad \forall v \in \mathbb{Z}$$

④ $f : \mathbb{Z}^3 \to \mathbb{Z}^4$

$$\begin{pmatrix} 2 & 0 & 1 \\ -1 & 2 & 4 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix} = M$$

$\mathrm{Im} f \subset \mathbb{Z}^4 \Rightarrow \mathrm{Im} f =$ sous-groupe libre de rang ≤ 4

$\mathrm{Ker} f \subset \mathbb{Z}^3 \Rightarrow \mathrm{Ker} f =$ " " rang ≤ 3

$$\begin{pmatrix} 1 & 0 & 2 \\ 4 & 2 & -1 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix} \leadsto \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & -9 \\ 3 & 6 & -3 \\ 1 & -3 & -1 \end{pmatrix} \leadsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -9 \\ 0 & 6 & -3 \\ 0 & -3 & -1 \end{pmatrix}$$

$$\leadsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 15 \\ 0 & 0 & 29 \end{pmatrix} \leadsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & \frac{29}{15} \end{pmatrix} \leadsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$ est équivalente à M.

Reste à trouver ce que représente cette matrice pour $\mathrm{Ker} f$ et $\mathrm{Im} f$

a.b. ancienne base

$$\begin{array}{ccc} \mathbb{Z}^3 & \xrightarrow{f} & \mathbb{Z}^4 \\ \downarrow & & \downarrow \\ \mathbb{Z}^3 & \xrightarrow[f]{} & \mathbb{Z}^4 \end{array}$$

n.b. (e_1, e_2, e_3) — nouvelle base (f_1, f_2, f_3, f_4)

Dans ces nouvelles bases : $f(x_1 e_1 + x_2 e_2 + x_3 e_3) = x_1 f_1 + x_2 f_2 + x_3 f_3$

$\mathrm{Im} f$ est engendré par le système $\{f_1, f_2, f_3\}$, et est isomorphe à $\mathbb{Z}^3$.

$\boxed{\mathrm{Im} f \simeq \mathbb{Z}^3} \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times 0\mathbb{Z}$ en effet $\mathrm{Im} f = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} / \exists u, v, w / \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} u \\ v \\ w \\ 0 \end{pmatrix} \right\}$

(c.à.d, est de rang 3)

$$(u, v, w, 0) \qquad \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times 0\mathbb{Z}$$

$\mathrm{Ker} f = \{ x_1 e_1 + x_2 e_2 + x_3 e_3 \ / \ x_1 f_1 + x_2 f_2 + x_3 f_3 = 0 \}$

$$\Updownarrow$$

$$x_1 = x_2 = x_3 = 0$$

Donc $\boxed{\operatorname{Ker} f = \{0\}}$

$\operatorname{Coker} f \doteq \mathbb{Z}^4 / \operatorname{Im} f$

pas évident

voir [2]

$$\mathbb{Z}^4/\operatorname{Im} f \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} / 1\mathbb{Z} \times 1\mathbb{Z} \times 1\mathbb{Z} \times 0\mathbb{Z} \simeq \underbrace{\mathbb{Z}/\mathbb{Z}}_{\{0\}} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \underbrace{\mathbb{Z}/0\mathbb{Z}}_{\mathbb{Z}}$$

$\simeq \mathbb{Z}$

$\simeq \mathbb{Z}$

~~Autre façon :~~

~~Présentation d'un sous-groupe (cf cours)~~

~~$\mathbb{Z}^4/\operatorname{Im} f \xrightarrow{\sim}$~~

⚠ On a : en général $H \simeq H' \not\Rightarrow G/H \simeq G/H'$

[1]

[2] Prendre, par exemple $\mathbb{Z}^2 / d_1\mathbb{Z} \times d_2\mathbb{Z} \xrightarrow[\sim]{\varphi} \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$

$$\dot{\overline{(x, y)}} \longmapsto (\dot{x}_{d_1}, \dot{y}_{d_2})$$

(5) $P_1(X) = 8X + 21$

$P_2(X) = 4X + 9$

$P_3(X) = 5X^2$

$P_4(X) = 7X^3 + 7X^4$

G est un groupe galtf et, dans la base canonique $(1, X, X^2, X^3, X^4)$ on a :

$$f : G \longrightarrow G$$

$$f = \begin{pmatrix} 21 & 9 & 0 & 0 \\ 8 & 4 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix} \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{matrix}$$

dans la base canonique)

On a $\mathrm{Im} f$ = groupe engendré par (P_1, P_2, P_3, P_4), par construction.

La question revient à déterminer, à un isomorphisme près, le conoyau de f :

$$\mathrm{Coker} f = G / \mathrm{Im} f \simeq ?$$

fait comme dans l'exercice précédent.

$$\begin{pmatrix} \not{21} \\ 8 \end{pmatrix} \quad f \rightsquigarrow \begin{pmatrix} 5 & 1 & 0 & 0 \\ 8 & 4 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 5 & 0 & 0 \\ 4 & 8 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & \not{7}\ 0 \end{pmatrix}$$

(remarquer : ce n'est pas la forme canonique, car $d_i \nmid d_{i+1}$!)

Donc $\operatorname{Im} f \simeq \mathbb{Z} \times 12\mathbb{Z} \times 5\mathbb{Z} \times 7\mathbb{Z} \times 0\mathbb{Z}$

$$G/_{\operatorname{Im} f} \simeq \mathbb{Z}^5 / \mathbb{Z} \times 12\mathbb{Z} \times 5\mathbb{Z} \times 7\mathbb{Z} \times 0\mathbb{Z}$$

important.

$$\simeq \underbrace{\mathbb{Z}/\mathbb{Z}}_{\{0\}} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \underbrace{\mathbb{Z}/0\mathbb{Z}}_{\mathbb{Z}}$$

(voir cours).

$$\boxed{G/_{\operatorname{Im} f} \simeq \mathbb{Z}/420\mathbb{Z} \times \mathbb{Z}}$$

(NB : en général $H, F \subset G$, $H \simeq F \not\Rightarrow G/_H \simeq G/_F$)

__Remarque__ :

Si l'on veut la "forme canonique" de la matrice de f :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & \overset{\text{problème}}{0} \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 15 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

on change un 0 en un nbre ≠ 0

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 7 & -35 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & -35 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 420 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(6) $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ CNS $\mathbb{Z}^2/_{\mathrm{Im} f}$ cyclique.

On sait que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ où $\left\{ d_1 \right.$

où $d_1 | d_2$

d'où $\mathrm{Coker} f = \mathbb{Z}^2/_{\mathrm{Im} f} = \mathbb{Z}^2/_{d_1\mathbb{Z} \times d_2\mathbb{Z}} \simeq \mathbb{Z}/_{d_1\mathbb{Z}} \times \mathbb{Z}/_{d_2\mathbb{Z}}$

* Si $d_1 d_2 \neq 0$ $\mathbb{Z}^2/_{\mathrm{Im} f}$ est cyclique ssi $\delta(d_1, d_2) = 1$ (théorème Chinois)

Alors $d_1 | d_2 \Rightarrow \{\delta(d_1, d_2) = 1$ ssi $d_1 = 1\}$

* Si $d_1 = 0 = d_2$, alors $f = \bar{0}$ et $\mathrm{Im} f = \{0\} \Rightarrow \mathbb{Z}^2/_{\mathrm{Im} f} \simeq \mathbb{Z}^2$ ~~cyclique~~ non cyclique.

* Si ~~d_1~~ $d_2 = 0$ et $d_1 \neq 0$ (l'autre cas est impossible car $d_1 | d_2$)

$\mathbb{Z}^2/_{\mathrm{Im} f} \simeq \underbrace{\mathbb{Z}/_{d_1\mathbb{Z}}}_{} \times \mathbb{Z}$

s'il était cyclique, il serait de la forme $\mathbb{Z}/_{d\mathbb{Z}}$ ou $\mathbb{Z}$.

Il ne peut être isomorphe à $\mathbb{Z}/_{d\mathbb{Z}}$ car $\mathbb{Z}/_{d\mathbb{Z}}$ est fini.

Il ne peut être isomorphe à $\mathbb{Z}$ car il possède des éléments d'ordre fini dans $\mathbb{Z}/_{d_1\mathbb{Z}}$, si $d_1 \neq 1$

Ainsi $\begin{cases} d_1 = 1 & \mathbb{Z}^2/_{\mathrm{Im} f} \text{ est cyclique} \\ d_1 \neq 1 & \mathbb{Z}^2/_{\mathrm{Im} f} \text{ non cyclique} \end{cases}$ $(d_2 = 0)$

Conclusion :

$$\boxed{\mathbb{Z}^2/\mathrm{Im} f \text{ est cyclique ssi } d_1 = 1 = \Delta(a,b,c,d)}$$

Application

$$\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ -6 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

$\delta(2,12) = 2 \neq 1 \Rightarrow \mathbb{Z}^2/\mathrm{Im} f$ n'est pas cyclique.

Mais $\mathbb{Z}^2/\mathrm{Im} f \simeq \mathbb{Z}^2/2\mathbb{Z} \times 12\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Si on décompose en composantes primaire le sous-groupe $\mathbb{Z}^2/\mathrm{Im} f$, on trouve :

$$\mathbb{Z}^2/\mathrm{Im} f \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\times 4\mathbb{Z} \simeq \underbrace{\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\right)}_{G(2)} \times \underbrace{\mathbb{Z}/3\mathbb{Z}}_{G(3)}$$

⑦ $\mathcal{U}(\mathbb{Z}/17\mathbb{Z})$ est un groupe multiplicatif abélien. Il est cyclique car $\mathbb{Z}/17\mathbb{Z}$ est un corps fini, à 16 éléments.

Quels sont les ordres possibles : 1, 2, 4, 8, 16

$\mathcal{U}(\mathbb{Z}/17\mathbb{Z}) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

x	$\omega(x)$
$\dot{1}$	1
$\dot{2}$	8
$\dot{3}$	16

$\dot{2}$, $\omega = 8$ → car $\dot{2}$ $\dot{4}$ $\dot{8}$ $-\dot{1}$ et $(-1)^2=1$ donc c'est 16.

$\dot{3}$, $\omega = 16$ → car $\dot{3}$ $\dot{9}$ $\dot{10}$ $-\dot{4}$ (soit 3^2, 3^3, 3^4)

donc $\omega(\dot{3}) \neq 2$ et 4.

et $\dot{3}^8 = (\dot{3}^4)^2 = \dot{16} \neq 1$

donc $\omega(\dot{3}) = 16$.

- Le nombre de générateurs de $U(\mathbb{Z}/_{17\mathbb{Z}})$ est égal au nbre de générateurs de $\mathbb{Z}/_{16\mathbb{Z}}$, c.à.d $\varphi(16) = \varphi(2^4) = 2^3 = 8$

<u>Trouvons les autres générateurs.</u>

On a : $U(\mathbb{Z}/_{17\mathbb{Z}}) = \{ \dot{3}^k \ / \ 0 \leq k \leq 16 \}$

- $\dot{3}^k$ engendre $U(\mathbb{Z}/_{17\mathbb{Z}}) \Leftrightarrow \Delta(k, 16) = 1$

en effet :

$$\varphi : \mathbb{Z}/_{16\mathbb{Z}} \xrightarrow{\sim} U(\mathbb{Z}/_{17\mathbb{Z}})$$
$$\dot{k} \longmapsto \dot{3}^k$$

cela provient de ($\dot{3}$ générateur de $U(\mathbb{Z}/_{17\mathbb{Z}})$, $\dot{1}$ générateur de $\mathbb{Z}/_{16\mathbb{Z}}$)

et pour trouver tous les générateurs de $U(\mathbb{Z}/_{17\mathbb{Z}})$, il faut et il suffit de trouver les générateurs de $\mathbb{Z}/_{16\mathbb{Z}}$, c.à.d les $\dot{k} \in \mathbb{Z}/_{16\mathbb{Z}}$ tels que

$\Delta(k, 16) = 1$

$\Updownarrow$

k impair.

Les huit générateurs de $\mathcal{U}(\mathbb{Z}/17\mathbb{Z})$ sont

$$\{\dot{3}, \dot{10}, \dot{5}, \dot{11}, \dot{14}, \dot{7}, \dot{12}, \dot{6}\}$$
$$\dot{10} = \dot{3}^3, \quad \dot{5} = \dot{3}^5$$

Moralité : quand on ~~or~~ a trouvé 1 générateur, on en déduit tous les autres.

(8) $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^k$ (1)

Soit
$$n = 2^\alpha \prod p_i^{\alpha_i} \qquad p_i \neq 2$$
la décomposition de n en facteurs premiers.

Le théorème chinois nous donne $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/2^\alpha\mathbb{Z} \times \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ (isomorphisme d'anneaux)

et (on l'a déjà utilisé) $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z}) \times$ ~~et~~ $\prod \mathcal{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$
(m̂ isomorphisme)

1) Si $\alpha = 0$

Alors $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}$ (voir cours) $\mathcal{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ cyclique, si $p_i \neq 2$) p_i premier

2) Si $\alpha = 1$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \underbrace{\mathcal{U}(\mathbb{Z}/2\mathbb{Z})}_{\{\dot{1}\}} \times \prod_i \mathbb{Z}/p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}$$

$$\simeq \prod_i \mathbb{Z}/p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}$$

3) Si $\alpha = 2$

Comme $\mathcal{U}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ ~~$\times \mathbb{Z}/2\mathbb{Z}$~~, on obtient

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\alpha_i - 1}(p_i - 1)\mathbb{Z}$$

4) Si $\alpha > 2$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\alpha_i - 1}(p_i - 1)\mathbb{Z}$$

●

Revenons à notre second terme :

Dans $(\mathbb{Z}/2\mathbb{Z})^k$, tout élément doit être d'ordre 2 au plus.

Si $\alpha \geq 4$, $\exists$, dans $\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$, des éléments d'ordre supérieur à 2

$\Downarrow$

$2^{\alpha - 2} \geq 2^2 > 2$

● Ainsi, si $\alpha \geq 4$, il n'y a pas de solution pour (1). Le seul cas intéressant pour le 4) est que $\alpha = 3$

4*) Si $\alpha = 3$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\alpha_i - 1}(p_i - 1)\mathbb{Z}$$

Le premier facteur, dans les trois cas, est toujours de la forme $(\mathbb{Z}/2\mathbb{Z})^k$ où $k = 0, 1, 2$.

Passons au 2-facteur : $\alpha_i \geq 2 \Rightarrow p_i | p_i^{\alpha_i - 1}(p_i - 1)$

donc p_i divise le cardinal de $\mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}}$

$$\Downarrow$$

$\exists x \in \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}}$ d'ordre $p_i > 2$.

Mais il n'y a pas de solution à (1)

Donc $\alpha_i = 1$. $(\forall i \in I)$

les seconds facteurs sont de la forme $\mathbb{Z}/_{(p_i-1)\mathbb{Z}}$. Il existe $x \in \mathbb{Z}/_{(p_i-1)\mathbb{Z}}$ ayant pour ordre $p_i - 1$. Donc, il existe un élément d'ordre $p_i - 1$ dans $\mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}})$ qui ne peut contenir que des éléments d'ordre ≤ 2. Donc $p_i - 1 \leq 2 \Leftrightarrow p_i = 3$ (car $p_i \neq 2$, si $p_i = 0$, on n'écrit pas le nbre premier dans la décomposition de n en nbres premiers.

Donc $n = 2^\alpha \quad 3 \times 2^\alpha \quad (\alpha \leq 3)$

~~Pour~~

c.à.d $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

$k \in \{0, 0, 1, 1, 1, 2, 2, 3\}$ construit à partir de $\varphi(n) = 2^k$

$$\Uparrow$$

$$\mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) \simeq (\mathbb{Z}/_{2\mathbb{Z}})^k$$

Remarque : $\mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) \simeq (\mathbb{Z}/_{2\mathbb{Z}})^k \Rightarrow \varphi(n) = 2^k$, réciproque fausse comme vous pouvez vous y attendre.

⑨ $(n^2+1)x - (n+1)y = 1$ résoluble dans $\mathbb{Z}$ $\Leftrightarrow$ n est pair

- Si n est impair, n^2+1 et $n+1$ sont pairs, absurde : $S = \emptyset$ (S ensemble des solutions)
- Supposons maintenant que n soit pair.

L'équation est résoluble ssi $\delta(n^2+1, n+1) = 1$. Montrons donc que n pair $\Rightarrow \delta(n^2+1, n+1) = 1$

Soit d diviseur commun à $n+1$ et n^2+1

Alors $d \mid (n+1)^2 = n^2+2n+1$ donc $d \mid 2n$

$$\left.\begin{array}{l} d \mid 2n \\ d \mid 2(n+1) \end{array}\right\} \Rightarrow d \mid 2 \Rightarrow d \in \{\pm 1, \pm 2\}.$$

$d = \pm 2$ impossible car $n+1$ impair.

Donc $d = \pm 1$.

Donc $\delta(n^2+1, n+1) = 1$. L'équation est résoluble dans $\mathbb{Z}$.

* Résolution $(n^2+1)x - (n+1)y = 1$

Sol. particulière :

n pair $n = 2q$. Supposons $n \geq 2$.

Alors $(n^2+1) = (n+1)(n-1) + 2$ $\quad 0 \leq 2 < n+1$

$n+1 = 2q+1$

d'où $(n^2+1)(-q) - (n+1)[-1-q(n-1)] = 1$ (1)

Résolution

$$\begin{cases} (n^2+1)x - (n+1)y = 1 \\ (n^2+1)x_0 - (n+1)y_0 = 1 \end{cases}$$

$(n^2+1)(x_0 - x) = (n+1)(y - y_0)$ et $\delta(n+1, n^2+1) = 1$ (cf(1))

Donc

$$\begin{cases} x_0 - x = (n+1)k \\ y_0 - y = (n^2+1)k \end{cases} \quad k \in \mathbb{Z}$$

$$\boxed{\begin{cases} x = x_0 - (n+1)k \\ y = y_0 - (n^2+1)k \end{cases} \quad k \in \mathbb{Z}}$$

(10) a) $\forall n \in \mathbb{Z} \quad 2730 \mid n^{13} - n$

b) $\forall n, m \in \mathbb{Z} \quad 56\ 786\ 730 \mid nm(n^{60} - m^{60})$ (Capes)

a) $n^{13} - n = n(n^{12} - 1) = n(n^6 + 1)(n^6 - 1)$

$= n(n^6 + 1)(n^3 + 1)(n - 1)(n^2 + n + 1)$

<u>Remarque</u> : $d \mid k \Rightarrow (n^d - 1) \mid (n^k - 1)$ $(\forall n \in \mathbb{N}^*)$

Preuve : On pose $k = hd$. Alors $(n^k - 1) = (n^{hd} - 1) = (n^d - 1)($ —— $)$

o .

On a $n^{13} - n = n(n^{\boxed{12}} - 1)$ ← k

Cherchons les diviseurs de 12 : $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$

Ainsi $\{n - 1, n^2 - 1, n^3 - 1, n^4 - 1, n^6 - 1, n^{12} - 1\}$ divisent $n^{13} - n$

On a

2730	2
1365	5
273	3
91	7
13	13
1	

Remarquons que : $\{1, 2, 3, 4, 6, 12\}$ = diviseurs de 12

$E = \{2, 3, ?, 5, 7, 13\}$ = décomp. de 2730 en nbres premiers

<u>Le théorème de Fermat</u> : $n^{p-1} \equiv 1 \; [p]$ $\begin{cases} \Delta(n,p) = 1 \\ p \text{ premier} \end{cases}$

preuve : $\# \mathcal{U}(\mathbb{Z}/p\mathbb{Z}) = p - 1$

si $\dot{n} \neq \dot{0}$, $n^{p-1} = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. (Facile)

$\Updownarrow$

$n \neq kp$ $\quad n^{p-1} \equiv$

$\forall p \in E, \quad n^p \equiv n \; [p]$

$\Updownarrow$

$n^p - n \equiv 0 \; [p]$ (1) vraie ssi $\delta(n,p) = 1$

$n(n^{p-1} - 1) \equiv 0 \; [p]$ (1') vraie $\forall n$, cette fois-ci)

Or $p-1$ est un diviseur de 12, donc $n^{p-1} - 1 \mid n^{12} - 1$

$\Downarrow$

$n^p - n \mid n^{13} - n$ (2)

Traduisons :

(1) $\Rightarrow p \mid n^p - n$

(2) $\Rightarrow n^p - n \mid n^{13} - n$

$\Rightarrow p \mid n^{13} - n$ ceci $\forall p \in E$

$\Downarrow$

$2730 \mid n^{13} - n$

b)

diviseurs de 60 $= \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ d

fct. premiers $= \{2, 3, \times, 5, \times, 7, 11, 13, \times, \times, 31, 61\}$ $\downarrow$ $d+1 = p$

Mais le problème est un peu différent.

Si $d \mid 60 \Rightarrow n^d - m^d \mid n^{60} - m^{60}$

$p = d+1$ $\begin{cases} n^d \equiv 1 \; [p] & \text{si } \delta(p,n) = 1 \\ m^d \equiv 1 \; [p] & \text{si } \delta(p,m) = 1 \end{cases}$

d'où $n^d - m^d \equiv 0 \; [p] \Rightarrow p \mid n^{60} - m^{60} \Rightarrow p \mid nm(n^{60} - m^{60})$

Ainsi, si $\delta(p,n) = \delta(p,m) = 1$, alors $p \mid nm(n^{60} - m^{60})$

sinon, par exemple $\delta(p,n) = 1 \Rightarrow p \mid n \Rightarrow p \mid nm(n^{60} - m^{60})$

c'est plus rapide.

Dans tous les cas, $p \mid nm(n^{60} - m^{60})$ $\forall p$ facteur premier intervenant dans la déc. de 56 786 730

Donc $56\,786\,730 \mid mn(n^{60} - m^{60})$

CQFD

IMSP

Mathématiques

—

TD ALG 6

M1 UV Algèbre et Arithmétique

6.02.79

Feuille N° 6

—

× 1°) Soit k un corps à p^n éléments (p premier, $n \in \mathbb{N}$); on désigne par F l'ensemble des applications de k dans lui-même. Soit $\phi : k[X] \to F$ qui associe à un polynôme f la fonction polynôme correspondante.

Montrer que $\ker \phi$ est l'idéal de $k[X]$ engendré par $X^{p^n} - X$

En déduire que ϕ est surjective.

× 2°) Soit $P \in \mathbb{R}[X]$ un polynôme tel que pour tout $t \in \mathbb{R}$, $P(t) \geq 0$. Montrer qu'il existe deux polynômes R et S de $\mathbb{R}[X]$ tels que $P = R^2 + S^2$.

× 3°) Trouver les polynômes P à coefficients réels vérifiant

$$P(X^2) = P(X)\, P(X+1).$$

× 4°) Soit un polynôme $F(X) = X^3 - X - 1$. Combien possède-t-il de racines réelles ? Soit ω une racine réelle, montrer que $\omega \notin \mathbb{Q}$. Montrer que $\{1, \omega, \omega^2\}$ est une partie libre du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.

× 5°) Soit E l'espace vectoriel des polynômes réels (!) de

degré inférieur ou égal à n. Soit T l'application de E dans E défini par $T(f)=g$ où $g(x)=f(x+1)-f(x)$.

Que pouvez-vous dire de T ?

× 6°) Soit $ax^2+bx+c=0$ une équation dans laquelle a, b, c sont entiers et a et c non nuls. Démontrez que si une racine est rationnelle, alors l'un au moins des coefficients est pair.

× 7°) Soient a, b, c, d des entiers non nuls.

α) Montrer que $a^3+b^3+c^3 \equiv 0\ (7) \Rightarrow abc \equiv 0 (7)$.

β) Montrer que si $a^3+b^3+c^3+d^3 \equiv 0\ (7)$, on n'a pas nécessairement $abcd \equiv 0\ (7)$.

8°) Résolvez dans $\mathbb{Z}$ l'équation $x^2+y^2=z^2$. Montrez que $x^4+y^4=z^4$ n'a pas de solution dans $\mathbb{Z}$.

9°) Trouvez les p-composants de $\mathbb{Z}/_{16\mathbb{Z}}$, $\mathbb{Z}/_{24\mathbb{Z}}$, $\mathbb{Z}/_{n\mathbb{Z}}$.

10°) Trouvez les p-composants de $G = \mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_{15\mathbb{Z}} \times \mathbb{Z}/_{10\mathbb{Z}}$.

× 11°) Soit G un groupe commutatif d'ordre n. Montrez que si $n = \prod_i p_i$ (p_i premier et $i \neq j \Rightarrow p_i \neq p_j$) G est un groupe cyclique. Exemple ?

6.02.79

③ $P \in \mathbb{R}[X]$

$P(X^2) = P(X)P(X+1)$ (1)

1) $P(X) =$ Cte a $\Rightarrow a = a^2 \Rightarrow a = 1$ ou 0

2) $P(X) \neq$ Cte, Th. de d'Alembert $\Rightarrow$ Soit α une racine de $P(X)$. Alors α^2 aussi.

Pro | α racine $\Rightarrow \alpha^{2^n}$ racine $(n \in \mathbb{N})$

α racine $\Rightarrow (\alpha - 1)^2$ racine

Pro | α racine $\neq 0$, $\neq 1$ $\Rightarrow \alpha^{2^n} \neq \alpha^{2^k}$ si $k \neq n$

En effet $\exists k, n / \alpha^{2^n} = \alpha^{2^k} \Rightarrow |\alpha|^{2^n - 2^k} = 1 \Rightarrow |\alpha| = 1$

Ainsi : les seules racines de P sont 0, 1 ou $\alpha \in \mathbb{C}$ tel que $|\alpha| = 1$.

On remarque que, si $\alpha \in \mathbb{C} \setminus \{0,1\}$ $|\alpha| = 1$. Posons $\alpha = e^{i\theta}$.

Alors $(e^{i\theta} - 1)^2$ est racine, donc $|e^{i\theta} - 1| = 1 \Rightarrow (\cos\theta - 1)^2 + \sin^2\theta = 1$

$\Rightarrow 2 - 2\cos\theta = 1$

$\Rightarrow 2\cos\theta = 1 \Rightarrow \cos\theta = \frac{1}{2}$

$\Rightarrow \begin{cases} \theta = \frac{\pi}{3} \; [2\pi] \\ \text{ou} \\ \theta = -\frac{\pi}{3} \; [2\pi] \end{cases}$ (1)

Mais aussi $(e^{i2\theta} - 1)^2$ est racine. Les m-calculs donnent $\begin{cases} 2\theta = \frac{\pi}{3} \; [2\pi] \\ \text{ou} \\ 2\theta = -\frac{\pi}{3} \; [2\pi] \end{cases}$ (2)

(1) et (2) sont incompatibles.

Donc les seules ~~polynômes~~ racines de P ~~sa~~ sont <u>0 ou 1</u>, peut-être.

Posons :

$P(X) = kX^n (X-1)^m$ où $k^2 = k \Rightarrow k = 0$ ou $k = 1$

~~$P(X^2) = k X^{2n} (X^2 - 1)$~~^{m}

$$\begin{cases} P(X) = X^n (X-1)^m \\ P(X^2) = X^{2n}(X^2-1)^m \end{cases}$$

et $P(X+1) = (X+1)^n (X)^m$

On doit avoir : $X^{2n}(X^2-1)^m = X^n(X-1)^m X^m (X+1)^n$

$$X^{2n}(X-1)^m(X+1)^m = X^{n+m}(X-1)^m(X+1)^n$$ ← décomposition en polynômes irréductibles puisque de degré 1. Cette déc. est unique.

$$\Downarrow$$

$$\begin{cases} 2n = n+m \\ n = m \end{cases}$$

$$\Downarrow$$

$$n = m$$

Ainsi $\boxed{P(X) = X^n (X-1)^n}$

Remarque sur le 4°/ : Autre méthode : résolution de $X^3 - X - 1$

$\boxed{X^3 + pX + q = 0 \quad (1)}$

$X = u + v \quad (2)$

$u^3 + v^3 + \underbrace{(3uv + p)}(u+v) + q = 0$

Posons $3uv + p = 0 \quad (3)$

Alors (4) $\begin{cases} uv = -\dfrac{p}{3} \\ u^3 + v^3 = -q \end{cases}$

$\begin{cases} U = u^3 \\ V = v^3 \end{cases}$ d'où (4) $\begin{cases} UV = -\dfrac{p^3}{27} \\ U + V = -q \end{cases}$

Rappel : Soit k un corps. $\mathbb{Z} \xrightarrow{f} k$ morphisme de groupe pour +
$1 \longmapsto 1 = f(1)$

(on note 1 l'él. unité de k et 0 son el. neutre)

Il est aisé de vérifier que ce morphisme de groupe est aussi un morphisme d'anneau.

Considérons $\operatorname{Ker} f = p\mathbb{Z} \subset \mathbb{Z}$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & k \\ \pi \downarrow & & \uparrow i \\ \mathbb{Z}/p\mathbb{Z} & \xrightarrow[\tilde{f}]{\sim} & \boxed{\operatorname{Im} f} \end{array}$$

c'est un sous-anneau de k, il est donc intègre.

Donc $\mathbb{Z}/p\mathbb{Z}$ est ~~un corps~~ intègre $\Rightarrow p = 0$ ou p premier.

On note p la caractéristique du corps k. Ainsi, si k est fini, alors $p \neq 0$.

| $p = \operatorname{car}(k)$ $\qquad$ k fini $\Rightarrow p \neq 0$ |

Pro | Si $\operatorname{Card} k < \infty$, alors $\operatorname{Card} k = p^n$ (p premier et $n \in \mathbb{N}$)

$\operatorname{Card} k < \infty$. Soit p la caractéristique du corps k

Alors k est un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$, par $\mathbb{Z}/p\mathbb{Z} \times k \to k$

$$(\dot{\lambda}, x) \longmapsto \underbrace{\tilde{f}(\dot{\lambda})}_{\in k} \underbrace{x}_{\in k}$$

Comme il n'y a qu'un nbre fini de vecteurs dans k, k sera un espace vectoriel de dimension finie sur $\mathbb{Z}/p\mathbb{Z}$. Et donc, si $\dim k = n < \infty$.

$$k \underset{ev}{\simeq} (\mathbb{Z}/p\mathbb{Z})^n \Rightarrow \boxed{\operatorname{Card} k = p^n}$$

Pro | Si k est un corps fini, alors k est commutatif (Wedderburn)

(cf. Bonnier Réchard)

① $\#k = p^n$ $\quad F = k^k$

$$\Phi : k[X] \to F$$
$$f \mapsto \Phi(f) \quad \text{où, si } f = \sum_{i=0}^{\infty} a_i x^i$$
$$\Phi(f)(\lambda) = \sum_{i=0}^{\infty} a_i \lambda^i \doteqdot f(\lambda)$$

<u>Montrons que $\operatorname{Ker}\Phi = \{(X^{p^n} - X) f \,/\, f \in k[X]\}$</u>

$\operatorname{Ker}\Phi$ est un idéal.

Pro | $f \in k[X]$
$\dim_k k[X] / \underbrace{f k[X]}_{(f)} = \deg f$

Preuve : laissée au lecteur.

On remarque, par exemple, que $\mathbb{R}[X] / (X^2+1)\mathbb{R}[X] \simeq \mathbb{C}$

$$\dot{f} \longmapsto f(i)$$

$\exists\, g \in k[X] \;/\; \operatorname{Ker} \Phi = (g)$ (cf cours : K corps $\Leftrightarrow$ $K[X]$ principal)

et $\deg g = \operatorname{Min} \{ \deg f \;/\; f \neq 0 \text{ et } f \in \operatorname{Ker} \Phi \}$

On constate que $X^{p^n} - X \in \operatorname{Ker} \Phi$ puisque :

$\forall x \in k \quad \Phi(X^{p^n} - X)(x) = x^{p^n} - x = 0$ car $\begin{cases} \text{si } x = 0, \text{ c'est vrai.} \\ \text{si } x \neq 0, x \in k^* \text{ et } \# k^* = p^n - 1 \\ \quad \text{donc } x^{p^n - 1} = 1 \Rightarrow x^{p^n} = x \end{cases}$

donc $\Phi(X^{p^n} - X) = 0 \in k^k$

Ainsi $(X^{p^n} - X) \subset \operatorname{Ker} \Phi$.

A prouver : si $f \in \operatorname{Ker} \Phi$, $\deg f \geq p^n$.

$f \in \operatorname{Ker} \Phi \Leftrightarrow \forall x \in k \quad f(x) = 0$ donc f admet p^n racines,

et donc $\deg f \geq p^n$

En déduire que Φ est surjective.

Ainsi, d'après la proposition rappelée :

$$\dim_k k[X]/\operatorname{Ker} \Phi = p^n \quad \text{or} \quad \underbrace{k[X]/\operatorname{Ker} \Phi \simeq \operatorname{Im} \Phi \subset F}_{(1)}$$

(1) et $\begin{cases} \operatorname{Card} \underbrace{k[X]/\operatorname{Ker} \Phi}_{\text{espace vectoriel}} = (\# k)^{p^n} = (p^n)^{p^n} \Rightarrow \operatorname{Card} \operatorname{Im} \Phi = (p^n)^{p^n} \\ \text{et } \operatorname{Card} F = (p^n)^{p^n} \Rightarrow \operatorname{Im} \Phi = F \end{cases}$

↑ car $F = k^k$

Conséquence : dans un corps fini k, toute application de k dans lui-même est une application polynomiale.

Autre méthode.

$\forall f \in \mathrm{Ker}\,\Phi \quad f \neq 0 \quad \deg f \geq p^n$ (facile $f(x) = 0 \ \forall x \Rightarrow f$ admet p^n racines)

Soit $\mathrm{Ker}\,\Phi = (h) \Rightarrow \deg h \geq p^n$

Donc $k[X] / \mathrm{Ker}\,\Phi \simeq \mathrm{Im}\,\Phi \subset F \quad (1)$

~~$\# k[X] = (p^n)^{\deg h}$~~

$\dim_k k[X] / \mathrm{Ker}\,\Phi = \deg h \geq p^n \Longrightarrow \# \mathrm{Im}\,\Phi \geq (p^n)^{p^n}$

or $\# \mathrm{Im}\,\Phi \leq (p^n)^{p^n}$

$\Rightarrow \mathrm{Im}\,\Phi = F \quad (1)$

Φ

(2) $P \in \mathbb{R}[X] \quad \forall t \in \mathbb{R} \quad P(t) \geq 0 \quad (1)$

Montrer que : $\exists R, S \in \mathbb{R}[X] \ / \ P = R^2 + S^2$

Lemme : . Soit P qui vérifie (1).
. Si $P(a) = 0$, alors $P(X) = (X-a)^{2\lambda} Q(X)$ avec $Q(a) \neq 0$

Si $P(X) = (X-a)^{2\lambda+1} Q(X) \quad Q(a) \neq 0. \Rightarrow$ (1) Faux. Absurde.

$(X-a)^{2\lambda+1}$: pas de signe constant au voisinage de a.

$Q(X)$: possède un signe constant au voisinage de a

Soit $P = Q \prod_{1 \le i \le p} (X - a_i)^{2n_i}$ avec $Q(t) > 0 \quad \forall t \in \mathbb{R}$

Remarque :

$$(a^2+b^2)(c^2+d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$
$$= (ac-bd)^2 + (ad+bc)^2$$

donc le produit de sommes de 2 carrés est une somme de 2 carrés.

$$P(X) = Q(X) \prod_{i=1}^{p} (X - a_i)^{2n_i} \quad \text{où } Q(t) > 0 \quad (t \in \mathbb{R})$$

Les racines de Q sont $a_1, \dots, a_k, \bar{a}_1, \dots, \bar{a}_k$ (th. de d'Alembert).

Donc $Q(X) = A \prod_{i=1}^{k} (X - a_i)(X - \bar{a}_i) = A \prod_1^k (\underbrace{X^2 - 2\,\mathrm{Re}\,a_i X + |a_i|^2}_{X^2 - \alpha X + \beta})$

$$X^2 - \alpha X + \beta = \left(X - \frac{\alpha}{2}\right)^2 - \frac{\alpha^2}{4} + \beta = \left(X - \frac{\alpha}{2}\right)^2 + \underbrace{\frac{4\beta - \alpha^2}{4}}_{>0}$$

(sinon, il existerait des rac. réelles)

Donc Q = somme de 2 carrés. On utilise la remarque un grand nbre de fois (récurrence finie), et l'on obtient bien ~~$Q = P^2 +$~~, $P = R^2 + S^2$

2^e^ méthode

$P \in \mathbb{C}[X]$ $\quad P(X) = \underbrace{\prod_{1 \le i \le k} (X - a_i)^{2\alpha_i}}_{T^2} \prod_{1 \le j \le h} (X - b_j)(X - \bar{b}_j)$

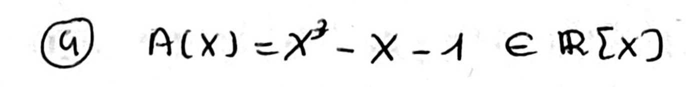
T^2 où $T = \prod_{1 \le i \le k} (X - a_i)^{\alpha_i}$

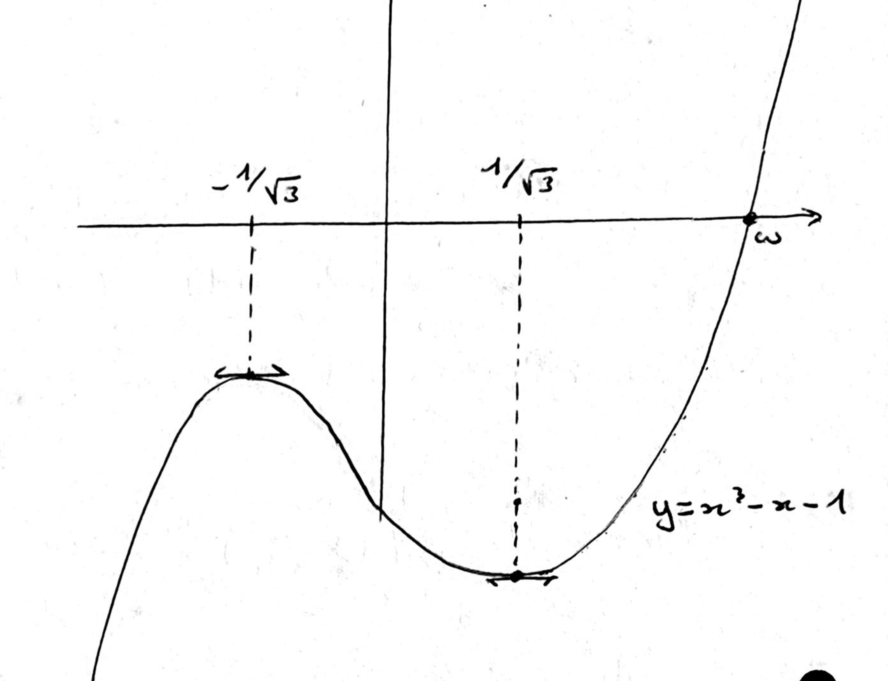
$$P(X) = T^2 S \bar{S} = (TS)(\overline{TS}) = Q \cdot \bar{Q} \quad \text{où } S = \prod_{1 \le j \le h} (X - b_j)$$

$Q = A + iB$ où $A, B \in \mathbb{R}[X]$ (lemme facile)

d'où $P(X) = (A + iB)(A - iB) = A^2 + B^2$ où $A, B \in \mathbb{R}[X]$

CQFD





Racines réelles ?

$f(x) = x^3 - x - 1$

x	$-\infty$		$-1/\sqrt{3}$		$1/\sqrt{3}$		$+\infty$
$f'(x)$		+	0	−	0	+	
$f(x)$		↗	α	↘	β	↗	

$\alpha = -\dfrac{1}{3^{\frac{3}{2}}} + \dfrac{1}{\sqrt{3}} - 1 \lessgtr 0$

Il n'existe qu'une seule racine réelle ω, et $\omega > \dfrac{1}{\sqrt{3}}$.

$\omega \notin \mathbb{Q}$

Si $\omega = \dfrac{p}{q}$ où $p, q \in \mathbb{Z}$ $\delta(p,q) = 1$

Alors $\omega^3 - \omega - 1 = 0 \Leftrightarrow p^3 - pq^2 - q^3 = 0 \Leftrightarrow p(p^2 - q^2) = q^3$

donc $p \mid q^3 \Rightarrow$ (th. gauss) $p \mid q$ car $\delta(p,q) = 1$.

~~C'est absurde car alors $\delta(p,q)$~~ $= p$.

Mais $p \mid q \Rightarrow \delta(p,q) = |p| = 1$

d'où $\omega = \dfrac{1}{q}$ et $1 - q^2 - q^3 = 0 \Rightarrow q^2(1+q) = 1$

$\Rightarrow q \mid 1 \Rightarrow q = \pm 1 \Rightarrow \omega = \pm 1$.

Il suffit de voir que $\omega \neq \pm 1$.

donc $\omega \notin \mathbb{Q}$.

CQFD

$\{1, \omega, \omega^2\}$ partie libre du $\mathbb{Q}$-ev $\mathbb{R}$.

$\alpha, \beta, \gamma \in \mathbb{Q}$ / $\alpha + \beta\omega + \gamma\omega^2 = 0$ (I)

Supposons que $\gamma \neq 0$.

Alors $\omega^2 = -\frac{1}{\gamma}(\alpha + \beta\omega)$

et, en reportant dans (II) : $\omega^3 - \omega - 1 = 0$, on trouve :

$$-\frac{1}{\gamma}(\alpha\omega + \beta\omega^2) - \omega - 1 = 0$$

$$\Updownarrow$$

$$-\frac{1}{\gamma}\left(\alpha\omega - \frac{\beta}{\gamma}(\alpha + \beta\omega)\right) - \omega - 1 = 0$$

$$\Updownarrow$$

$$\left(-1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2}\right)\omega + \frac{\alpha\beta}{\gamma^2} - 1 = 0 \qquad (1)$$

* Si $\left(-1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2}\right) = 0$, alors $\alpha\beta = \gamma^2$.

Ainsi $\begin{cases} \alpha\beta = \gamma^2 \Rightarrow \alpha\beta \neq 0 \\ \frac{\beta}{\alpha} = 1 + \frac{\alpha}{\gamma} \Rightarrow \left(\frac{\beta}{\alpha} - 1\right)^2 = \frac{\alpha^2}{\gamma^2} \Rightarrow \left(\frac{\beta}{\alpha} - 1\right)^2 = \frac{\alpha}{\beta} \end{cases}$

~~Posons $t = \frac{\alpha}{\beta} \in \mathbb{Q}$~~

On peut prendre $\alpha = 1$ $\begin{cases} \gamma^2 = \beta \\ \beta^2 = \gamma^2 + \gamma \end{cases} \Rightarrow \begin{cases} \gamma^4 = \gamma^2 + \gamma \\ \gamma^3 - \gamma - 1 = 0 \end{cases}$.

~~Alors $\left(\frac{1}{t} - 1\right)^2 = t \Leftrightarrow t^2 + t - 1 = 0 \Leftrightarrow t = \frac{-1 \pm \sqrt{5}}{2} \notin \mathbb{Q}$, absurde~~ ($\frac{1}{t}$)

cf. Autre solution : voir m̂ TD p. 8

Donc :

* $-1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2} \neq 0$. Mais alors (1) $\Rightarrow \omega \in \mathbb{Q}$, absurde.

Donc :

$\gamma = 0$

(I) devient $\alpha + \beta\omega = 0$. $\begin{cases} \beta \neq 0 \Rightarrow \omega = -\frac{\alpha}{\beta} \in \mathbb{Q}. \text{ Absurde} \\ \text{donc } \beta = 0 \Rightarrow \alpha = 0. \end{cases}$

CQFD

⑥ $x = \frac{p}{q}$ où $\delta(p,q) = 1$

$$a\frac{p^2}{q^2} + b\frac{p}{q} + c = 0$$

$$ap^2 + bpq + cq^2 = 0 \quad (I)$$

Alors $(ap+bq)p = -cq^2$ $c \neq 0$ $\Rightarrow$ $q \mid ap+bq \Rightarrow q \mid ap \Rightarrow q \mid a$ (Gauss).

Donc $a = \lambda q$

De la m̂ façon on montre que $c = \mu p$.

* Si p ou q pair, alors a ou c pair et c'est terminé.
* Supposons donc que p et q sont impairs. Alors (I) permet de conclure.

En effet : p^2 impair pq impair et q^2 impair.

Si a, b, et c impairs, alors $ap^2 + bpq + cq^2$ impair, absurde.

Donc a, ou b, ou c pair.

CQFD

⑦ $a, b, c, d \in \mathbb{Z}$

$$a^3 + b^3 + c^3 \equiv 0 \ [7] \Rightarrow abc \equiv 0 \ [7]$$

On constate que

$\dot{a} \neq \dot{0} \Rightarrow \dot{a}^3 = \pm 1$.

et que :

$\dot{a} \neq \dot{0}$ $\dot{b} \neq \dot{0}$ et $\dot{c} \neq \dot{0} \Rightarrow \dot{a}^3 + \dot{b}^3 + \dot{c}^3 \neq \dot{0}$.

Donc $\dot{a} = \dot{0}$ ou $\dot{b} = \dot{0}$ ou $\dot{c} = \dot{0}$

$(\mathbb{Z}/7\mathbb{Z})$

a	0	1	2	3	-3	-2	-1
a^2	0	1	-3	2	2	-3	1
a^3	0	1	1	-1	1	-1	-1

Le tableau nous donne aussi : $a = 1$ $b = 2$ $c = 3$ $d = -2$

$\dot{a}^3 + \dot{b}^3 + c^3 + d^3 \equiv 0$ et pourtant $abcd = -12 = 2 \neq 0$

On a : (1) et (2) $\Leftrightarrow$ (3) $\Rightarrow$ (4)

$\Updownarrow$

(4) et $uv = -\frac{p}{3}$

Prenons $p, q \in \mathbb{R}$ pour simplifier.

$$T^2 + qT - \frac{p^3}{27} = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = \frac{27q^2 + 4p^3}{27}$$ s'appelle le "discriminant" de (1).

C'est une définition bizarre, n'est-ce pas ?

$$\mathrm{Disc}(1) = 4p^3 + 27q^2$$

1) Si $\Delta > 0$

Alors $\exists\, U$ et $V \in \mathbb{R}$ avec $U = u^3$ et $V = v^3$ où $u, v \in \mathbb{R}$

Toutes les racines cubiques de U sont $\{u, ju, j^2u\}$

" " V sont $\{v, jv, j^2v\}$

On a $u^3v^3 = -\frac{p^3}{27} \Rightarrow uv = -\frac{p}{3}$ car u et v et p réels.

On a : "$\sqrt[3]{U}$" "$\sqrt[3]{V}$"

u — v

ju — j^2v

j^2u — jv

Les solutions sont donc $x = \begin{cases} u+v \\ ju + j^2v \\ j^2u + jv \end{cases}$ (car on a aussi la condition $uv = -\frac{p}{3} \in \mathbb{R}$

$u^3 \neq v^3$

$\Downarrow$

Si $u \neq v \Rightarrow x = \begin{cases} u+v \\ ju + j^2v \notin \mathbb{R} \\ j^2u + jv \notin \mathbb{R} \end{cases}$

Donc, si $\Delta > 0$, (1) n'admet qu'une racine réelle et a 2 racines conjuguées.

* $P = X^n + \lambda_1 X^{n-1} + \dots + \lambda_1$ où $Pk[X] = I$. Donc :

$P(\omega) = 0 = \omega^n + \lambda_1 \omega^{n-1} + \dots \Rightarrow \omega^n \in$ ev engendré par $(1, \omega, \dots, \omega^{n-1})$

Donc $\omega^{n+k} \in$ ev engendré $(1, \dots, \omega^{n-1})$

2- démonstration :

$$\Phi : k[X] \to K$$
$$f \longmapsto f(\omega)$$

Φ est une application k-linéaire de ces deux k-espaces vectoriels.

Et $\text{Im}\,\Phi$ = ensemble des ~~coefficients~~ combinaisons linéaires à coefficients dans k, de toutes les puissances de ω.

On a la décomposition canonique :

$$\begin{array}{ccc} k[X] & \xrightarrow{\Phi} & K \\ \downarrow & \nearrow & \uparrow \\ k[X]/\text{Ker}\,\Phi & \xrightarrow{\sim} & \text{Im}\,\Phi \end{array}$$

et $\dim k[X]/\underbrace{\text{Ker}\,\Phi}_{I} = \dim k[X]/Pk[X] = \deg P$

Donc $\boxed{\dim(\text{Im}\,\Phi) = \deg P.}$

Retournons à l'exo 4 :

$\mathbb{Q}, \mathbb{R}$

$\begin{cases} A = X^3 - X - 1 \\ A(\omega) = 0 \end{cases}$

Soit $I = \{ f \in \mathbb{Q}[X] \,/\, f(\omega) = 0 \}$

On a déjà $A \in I$

$I = P.\mathbb{Q}[X]$ où $P \in \mathbb{Q}[X]$

Donc $A \in I \Rightarrow A = PQ$

Si $\deg P \neq 3$, $\neq 0$ alors $\deg P$ ou $\deg Q = 1$ et donc P ou Q possède une racine rationnelle, donc A aussi, ce qui est absurde.

Donc $\deg P = 0$ ou $\deg P = 3$.

Si $\deg P = 0$, $P = 0$ (car $P(\omega) = 0$), alors $A = 0$ ce qui est faux car $A = X^3 - X - 1$

Donc $\deg P = 3$. $P = \text{cte } A$

$A = \text{cte} P \Rightarrow I = A.\mathbb{Q}[X]$

⑤ $E_n = \{ f \in \mathbb{R}[X] \ / \ \deg f \leq n \}$

$T : E_n \to E_n$

$f \mapsto T(f) = g$ où $g(X) = f(X+1) - f(X)$

* $\dim E_n = n+1$
* T est linéaire

[redacted]peut écrire $f(X+1) = f \circ L(X)$ où $L(X) = X+1$

où $\begin{cases} f = \sum_{i=0}^{n} a_i X^i \\ f \circ L = \sum_{i=0}^{n} a_i L^i \end{cases}$

Remarque : $f \in \mathbb{k}[X]$

$A \xrightarrow{f_*} A$ (A algèbre)

$s \mapsto \sum_{i=0}^{\infty} a_i s^i$

* Si $\deg P = n$, $n \neq 0$, alors $\deg T(P) = n - 1$

$$1 \overset{T}{\longmapsto} 0$$

$$X \longmapsto 1$$

$$X^2 \longmapsto 2X + 1$$

$$\vdots$$

$$X^n \longmapsto T(X^n) = (X+1)^n - X^n = nX^{n-1} + \dots$$

Ainsi, $\forall k \in [1, n]$ $\deg(T(X^k)) = k - 1$

Soit $P \in E_n$, $P = \sum_{i=0}^{k} a_i X^i \Rightarrow T(P) = \underbrace{a_k}_{\neq 0} T(X^k) + \underbrace{\dots + a_1 T(X)}_{\text{de degré} \leq n-1} + 0$

Noyau de T ?

$f \in E_n$ / $f(X+1) = f(X)$

$f \neq$ Cte $f \in \mathbb{R}[X] \Rightarrow \exists \alpha \in \mathbb{C}$ $f(\alpha) = 0$

Mais alors $\forall n \in \mathbb{N}$ $f(\alpha + n) = 0 \Rightarrow f$ admet une infinité de racines ($\mathbb{R}$ = anneau com. intègre infini $\Rightarrow f = 0$)

donc $\ker T = \{\text{Cte}\} \simeq \mathbb{R}$

Im T ?

$$E_n / E_0 \simeq \text{Im}\, T$$

$$\Downarrow$$

$\dim \text{Im}\, T = n$
Mais $\text{Im}\, T \subset E_{n-1}$ $\Big\} \Rightarrow \text{Im}\, T = E_{n-1}$

Application. (cf. Godement)

$$S_{n,m} = \sum_{1 \leq x \leq n} x^m$$

$\exists f \;/\; \deg f = m+1 \qquad f(X+1) - f(X) = X^m$

Alors
$$\begin{cases} 1^m = f(2) - f(1) \\ 2^m = f(3) - f(2) \\ \text{----} \\ n^m = f(n+1) - f(n) \end{cases}$$

$$S_{n,m} = f(n+1) - f(1)$$

Si $m = 2$, on calcule facilement $\sum_{x=1}^{n} x^2$

$f(X) = aX^3 + bX^2 + cX \quad \Rightarrow \quad T(f) = a[(X+1)^3 - X^3] + b[(X+1)^2 - X^2] + c[X+1-X]$

$T(f) = a(3X^2 + 3X + 1) + b(2X+1) + c = X^2$

$a = \frac{1}{3}$ donc $X^2 + X + \frac{1}{3} + b(2X+1) + c = X^2$

$b = -\frac{1}{2} \qquad \frac{1}{3} - \frac{1}{2} + c = 0 \Rightarrow c = \frac{1}{6}$

donc
$$\boxed{f(X) = \frac{1}{3}X^3 - \frac{1}{2}X^2 + \frac{1}{6}X}$$

D'où
$$\sum_{x=1}^{n} x^2 = \frac{1}{3}(n+1)^3 - \frac{1}{2}(n+1)^2 + \frac{1}{6}(n+1) - 0$$

$$\boxed{\sum_{x=1}^{n} x^2 = \frac{n(n+1)(2n+1)}{6}}$$

Remarques : 1)

$$f_k = \frac{X(X-1)\cdots(X-k+1)}{k!} = $$

$$T(f_k) = \frac{(X+1)X(X-1)\cdots(X-k+2) - X(X-1)\cdots(X-k+1)}{k!}$$

$$= \frac{X(X-1)\cdots(X-k+2)\,[\,\cancel{X}+\cancel{1} - \cancel{X} + k - \cancel{1}\,]}{k!}$$

$$= f_{k-1}$$

(cf. C_n^k)

2) $\begin{cases} T^k(f) = T(T^{k-1} f) \\ T^0 f = f \end{cases}$

$$f = \sum_{k=0}^{\infty} (T^k f)(0)\, f_k$$

(8) (grand théorème de Fermat : $x^n + y^n = z^n$ n'a pas de solutions pour $n \geq 3$)

$\boxed{x^2 + y^2 = z^2}$ (1) dans $\mathbb{N}$ (puisque après, c'est facile, dans $\mathbb{Z}$)

Soit $d = \delta(x, y, z)$ $\begin{cases} x = dx' \\ y = dy' \\ z = dz' \end{cases}$

Alors (1) $\Leftrightarrow$ $x'^2 + y'^2 = z'^2$ où $\delta(x', y', z') = 1$

Résoudre (1) équivaut à résoudre (2) : $\begin{cases} x^2 + y^2 = z^2 \\ \delta(x, y, z) = 1. \end{cases}$

Pro | Si $x^2+y^2=z^2$ et $\delta(x,y,z)=1$, alors x,y,z sont premiers entre eux deux à deux.

Si $\delta \mid x$ et $y \Rightarrow \delta^2 \mid z^2 \Rightarrow \delta \mid z \Rightarrow \delta = \pm 1$

Si z pair, alors z^2 est divisible par 4. Alors x et y impairs, donc $x^2+y^2=4u+2$ d'où $x^2+y^2 \equiv 2\ [4]$ et $z^2 \equiv 0\ [4]$, donc z pair ne peut être solution.
Donc, forcément z est impair.

Donc x et y ont des parités différentes. Supposons que x soit impair et y pair (Symétrie entre x et y)

1^re méthode : Solution algébrique.

$y^2 = z^2 - x^2 = (z-x)(z+x)$

$\delta = \delta(z-x, z+x) \Rightarrow \delta \mid \begin{matrix} 2z \\ 2x \end{matrix}$

Comme $z-x$ et $z+x$ pair, $\delta = 2\delta' \Rightarrow \delta' \mid \begin{matrix} x \\ z \end{matrix} \Rightarrow \delta' = 1$ car $\delta(x,z)=1$

Donc $\delta(z-x, z+x) = 2$

On écrit :

$$\frac{y^2}{4} = \frac{z-x}{2} \cdot \frac{z+x}{2} \quad \text{et} \quad \delta\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$$

$\frac{y^2}{4} = \left(\frac{y}{2}\right)^2$

lemme | $a^2 = uv \quad \delta(u,v)=1$
Alors $\exists\, \alpha, \beta \quad u=\alpha^2 \quad v=\beta^2$

Preuve $\delta = \delta(a,u) \quad a=\delta a' \quad u=\delta u' \quad \delta(a',u')=1$

$\delta^2 a'^2 = \delta u' v \Rightarrow \delta a'^2 = u'v \Rightarrow u' \mid \delta a'^2 \Rightarrow u' \mid \delta$ (Gauss) on note $\delta = u'\delta'$

d'où $\delta' \not{u'} a'^2 = \not{u'} v \Rightarrow \delta' | v$

or $\delta' | \delta | u \Rightarrow \delta' | u \Rightarrow \left.\begin{matrix}\delta' | u \\ \delta' | v\end{matrix}\right\} \Rightarrow \delta' = 1$

D'où $a'^2 = v$

et $\delta = u'$ et $u = u'^2$

CQFD

(NB : 2– dém. avec les valuations)

Par application de ce lemme : $\exists \alpha, \beta$ $\left\{\begin{matrix}\frac{z-x}{2} = \alpha^2 \\ \frac{z+x}{2} = \beta^2\end{matrix}\right.$

$\left\{\begin{matrix}z - x = 2\alpha^2 \\ z + x = 2\beta^2\end{matrix}\right. \Rightarrow \left\{\begin{matrix}z = \alpha^2 + \beta^2 \\ x = \beta^2 - \alpha^2\end{matrix}\right.$

d'où $y = \sqrt{z^2 - x^2} = 2\alpha\beta$

$\left\{\begin{matrix}x = \beta^2 - \alpha^2 \\ y = 2\alpha\beta \\ z = \alpha^2 + \beta^2\end{matrix}\right.$ $\delta(\alpha, \beta) = 1$ et $\alpha \not\equiv \beta$ [2] car x impair.

$\Uparrow$ $\Downarrow$

$x^2 + y^2 = z^2$ (x impair, y pair) $\delta(x, y, z) = 1$

$\Downarrow$ * $\left\{\begin{matrix}x^2 + y^2 = \beta^4 + \alpha^4 - 2\alpha^2\beta^2 + 4\alpha^2\beta^2 = (\alpha^2 + \beta^2)^2 = z^2 \\ z^2 = (\alpha^2 + \beta^2)^2\end{matrix}\right.$ oui.

* $\left|\begin{matrix}x \text{ impair.} \\ y \text{ pair}\end{matrix}\right.$ évident.

* Enfin $\delta(x, y, z) = 1$ puisque, si d est un diviseur commun à $\beta^2 - \alpha^2$

$2\alpha\beta$ et $\alpha^2+\beta^2$

Alors $d \mid 2\beta^2$ $\quad d \mid 2\alpha^2$ $\quad$ et $d \mid 2\alpha\beta$.

d n'est pas pair car $d \mid \underbrace{\beta^2-\alpha^2}_{\text{impair}}$. Donc $\delta(d,2)=1 \Rightarrow \begin{cases} d \mid \alpha^2 \\ d \mid \beta^2 \end{cases}$ et $d \mid \alpha\beta$

$\Downarrow$

$d = 1$

(car $\delta(\alpha^2,\beta^2)=1$)

- Solutions classiques : $\begin{cases} x = 3 \\ y = 4 \\ z = 5 \end{cases}$

Y-a-t'il plus de solutions consécutives ?

$n^2 + (n+1)^2 = (n+2)^2$

$n^2 - 2n - 3 = 0$

$\Delta' = 1 + 3 = 4$

$1 \pm 2 \; \Big| \begin{matrix} 3 \\ -1 \end{matrix}$

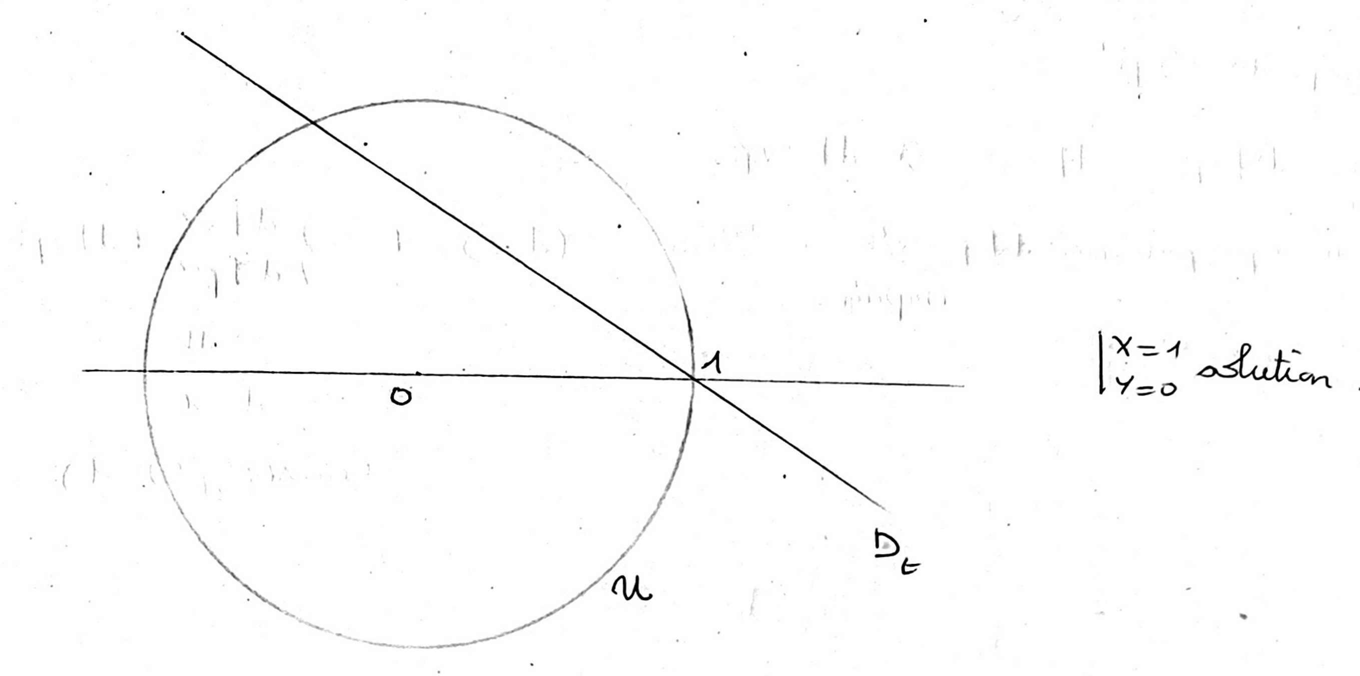
- $(n+1)(n-3) = 0 \quad \Rightarrow \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ +1 \end{pmatrix}$ ou $\begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$

2-méthode : Solution géométrique.

$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$

$X^2 + Y^2 = 1$

Problème : trouver les pts à coordonnées rationnelles sur le cercle unité $\mathcal{U}$.



$\left| \begin{array}{l} X=1 \\ Y=0 \end{array} \right.$ solution.

$Y = t(1-X)$

Cherchons $D_t \cap \mathcal{U}$: $t^2(1-X)^2 = (1-X^2)$

$\Downarrow$

$t^2(1-X) = 1+X \qquad (t \neq 1)$

$\Downarrow$

$X(1+t^2) = t^2-1$

$\Downarrow$

$$\begin{cases} X = \dfrac{t^2-1}{t^2+1} = \dfrac{x}{z} \\ Y = \dfrac{2t}{t^2+1} = \dfrac{y}{z} \end{cases}$$

Ainsi, si $t \in \mathbb{Q}$ $t = \frac{p}{q}$ $\delta(p,q) = 1$

et $\begin{cases} x = \dfrac{p^2-q^2}{p^2+q^2} z \\ y = \dfrac{2pq}{p^2+q^2} z \end{cases}$ On a choisi, rappelons le, $\begin{pmatrix} x \text{ impair} \\ y \text{ pair} \\ \delta(x,y,z) = 1 \end{pmatrix}$

$d = \delta(p^2+q^2, p^2-q^2)$, alors $d \mid 2p^2$ et $d \mid 2q^2 \Rightarrow d = 1$ ou 2.
(si d impair...
si d pair...)

① $d = 1 \Rightarrow p^2+q^2 \mid (p^2-q^2)z \Rightarrow \begin{cases} z = \lambda(p^2+q^2) \\ x = \lambda(p^2-q^2) \end{cases} \Rightarrow \lambda = 1 \Rightarrow \begin{cases} z = p^2+q^2 \\ x = p^2-q^2 \\ y = 2pq \end{cases}$

12

② $d = 2 \Rightarrow p$ et q impairs $\Rightarrow x$ est pair (car $p^2 - q^2 \equiv 0 [4]$)

donc x divisible par 4

Or $p^2 + q^2$ est divisible par 2, mais pas plus.

Donc x pair, c'est absurde.

Remarque :

$\mathbb{Z}[i] = \{a + ib \,/\, a, b \in \mathbb{Z}\}$ est un anneau euclidien.

$\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

A prouver : $x^4 + y^4 = z^2$ non résoluble avec $x, y, z > 0$

$\Downarrow$

non plus $x^4 + y^4 = z^4$.

Preuve : Soit $d = \Delta(x, y, z)$ $\begin{cases} x = dx' \\ y = dy' \\ z = dz' \end{cases}$

$$d^4(x'^4 + y'^4) = d^2 z'^2$$

$$d^2(x'^4 + y'^4) = z'^2$$

donc $d^2 | z'^2 \Rightarrow d | z' \Rightarrow z' = dz''$

$$x'^4 + y'^4$$

lemme : $d^2 | z'^2 \Rightarrow$ ~~z~~ $d | z'$

Preuve : $\delta = \Delta(d, z')$ $\begin{cases} d = \delta d' \\ z' = \delta z'' \end{cases}$ ~~$\Rightarrow \delta^2$~~

D'où $\delta^2 z''^2 = \lambda \delta^2 d'^2 \Rightarrow z''^2 = \lambda d'^2$, $\Delta(d', z'') = 1$ $\Big\}$ $\Rightarrow d' | z''^2$

$\Rightarrow d' | z''$ (lemme de gauss)

$\Rightarrow d' = 1$

donc $d | z'$

d'où $x'^4 + y'^4 = z''^2$ où $\delta(x', y', z'') = 1$

premiers dans leur ensemble

$$\begin{cases} x'^2 = \alpha^2 - \beta^2 \\ y'^2 = 2\alpha\beta \\ z'' = \alpha^2 + \beta^2 \end{cases} \Rightarrow x'^2 + \beta^2 = \alpha^2 \Leftrightarrow \begin{cases} x' = u^2 - v^2 \\ \beta = 2uv \text{ (forcément pair)} \\ \alpha = u^2 + v^2 \end{cases}$$

où $\delta(\alpha, \beta) = 1$ → et $\delta(x', \alpha, \beta) = 1$

où $\delta(u, v) = 1$

Donc $y'^2 = 4\alpha uv \Rightarrow \alpha uv$ est un carré

$\Downarrow$ α, u et v sont premiers entre eux deux à deux ($\exists p \in \mathcal{P}$ $p | \alpha$ et u, alors $p | v^2 \Rightarrow p | v \Rightarrow p = 1$. Donc $\nexists p \in \mathcal{P}$ $p | \alpha$ et u $\Downarrow$ $1 = \delta(\alpha, u)$)

α, u et v sont des carrés.

On peut écrire $\begin{cases} \alpha = A^2 \\ u = U^2 \\ v = V^2 \end{cases}$

d'où $A^2 = U^4 + V^4$

on avait $\delta(u, v) = 1 \Rightarrow \delta(U, V) = 1$

donc $\delta(A, U, V) = 1$.

Je prétends que les solutions de cette équation sont plus petites que les solutions précédentes :

On a $0 < A < z'$ puisque $A = \sqrt{\alpha} \leq \alpha \leq \alpha^2 < z$

car $z = \alpha^2 + \beta^2$

On suppose $\exists$ sol $x^4+y^4=z^2$ (>0)

$z_1 = \text{Inf}\ \{z>0 \ / \ \exists x,y \ / \ x^4+y^4=z^2\} > 0$

Mais on sait fabriquer une solution A plus petite, ce qui contredit $z_1 = \text{Inf}\{\ \}$. Donc $\nexists$ solution $x^4+y^4=z^2$. CQFD

(Procédé de descente infinie de Fermat)

(11) G = groupe commutatif d'ordre n ⇒ G cyclique.
où $n = \prod_{i=1}^{I} p_i$

$n = \prod_{i=1}^{I} p_i$ G est un gatf et donc $G \simeq \prod_{j=1}^{k} \mathbb{Z}/d_j\mathbb{Z}$ où $d_j | d_{j+1}$

On a $d_1 \dots d_k = n$ (1)

(1) ⇒ $d_1 | n \Rightarrow d_1 = \prod_{i=1}^{I} p_i^{\alpha_i^1}$ où $\alpha_i^1 = 1$ ou 0.

$d_1 | d_2 | n \Rightarrow d_2 = \prod_{i=1}^{I} p_i^{\alpha_i^2}$ où $\alpha_i^2 = 1$ ou 0 et $\alpha_i^2 \geq \alpha_i^1$

-.- - - - -

$d_1 | \dots | d_k | n \Rightarrow d_k = \prod_{i=1}^{I} p_i^{\alpha_i^k}$ où $\alpha_i^k \geq \alpha_i^{k-1} \geq \dots \geq \alpha_i^1$

De plus, (1) ⇒ $\sum_{j=1}^{k} \alpha_i^j = 1$ $(\forall i)$ (2)

Si $\exists i \in [1, I]$ / $\exists j \in [1, k[$ $\alpha_i^j = 1$

alors $\alpha_i^k \geq \alpha_i^{k-1} \geq \dots \geq \alpha_i^j = 1 \Rightarrow \alpha_i^k = \dots = \alpha_i^j = 1$

donc $\sum_{j=1}^{k} \alpha_i^j \geq 2$, impossible

Donc : $\forall i \in [1, I]$ $\forall j \in [1, k[$ $\alpha_i^j = 0$

⇓

$$\begin{cases} d_1 = \dots = d_{k-1} = 1 \\ \text{et } d_k = \prod_{i=1}^{I} p_i = n \end{cases}$$

D'où $G \simeq \mathbb{Z}/\mathbb{Z} \times \dots \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$

CQFD

$$\begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ v(e_3) = e_4 = v^2(e_2) \\ v(e_4) = 0 \end{cases}$$

$v^3 = 0$

$\operatorname{Ker} v \underset{\neq}{\subset} \operatorname{Ker} v^2 \underset{\neq}{\subset} \operatorname{Ker} v^3 = E$

car $(X-1)^2 \times \left[K[X]/(X-1) \times K[X]/(X-1)^3 \right] \neq 0 \ \forall x$.

(car $\operatorname{Ker} v = \operatorname{Ker} v^2 \Rightarrow \operatorname{Ker} v^2 = \operatorname{Ker} v^3$.)

~~Si l'on calc~~

On sait que $\left.\begin{array}{l} \dim \operatorname{Ker} v = 2 \\ \dim \operatorname{Ker} v^3 = 4 \end{array}\right\} \Rightarrow 2 < \dim \operatorname{Ker} v^2 < 4 \Rightarrow \dim \operatorname{Ker} v^2 = 3$.

Prenons $\begin{cases} e_2 \notin \operatorname{Ker} v^2 \\ e_2 \neq 0 \\ e_3 = v(e_2) \\ e_4 = v(e_3) \end{cases}$

~~Cette base~~

Ce système (e_2, e_3, e_4) est libre car $\lambda_2 e_2 + \lambda_3 e_3 + \lambda_4 e_4 = 0$

$$\Downarrow$$

$$\lambda_2 = \lambda_3 = \lambda_4 = 0$$

On prend $e_1 \in$ (supplémentaire de e_4 dans $\operatorname{Ker} v$).

Alors (e_1, e_2, e_3, e_4) = base telle que $\begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ v(e_3) = e_4 \\ v(e_4) = 0 \end{cases}$

d) $\begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix} = u$ ~~est semblable à~~ ~~se équivalente à~~ $\begin{pmatrix} 1 & & \\ & & \\ & & \end{pmatrix}$ ~~$X-2$~~

$E \simeq K[X] / (X-2)$

u est semblable à $w = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$

car $u - XI$ est équivalente à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$

Base où cette matrice se met sous forme de Jordan.

Posons $\begin{cases} v = u - 2I \\ v^2 = 0 \end{cases}$

Problème : Trouver (e_1, e_2, e_3) tels que $\begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ \Downarrow \\ v(e_3) = 0 \end{cases}$

Trouver $v(e_2) \neq 0$?

$e_2 \notin \operatorname{Ker} v$, si $e_2(x, y, z)$ ~~avec~~ :

$\begin{cases} 4x + 20y - 34z \neq 0 \\ 6x + 30y - 51z \neq 0 \\ 4x + 20y - 34z \neq 0 \end{cases}$ Prenons $\boxed{e_2 (1, 0, 0)}$

Prenons $\boxed{e_3 = v(e_2) = \begin{pmatrix} 4 \\ 6 \\ 4 \end{pmatrix}}$

Noyau de v ? $\begin{cases} 4x + 20y - 34z = 0 \\ 6x + 30y - 51z = 0 \end{cases} = (\operatorname{Ker} v.)$

Prenons e_1 dans $\operatorname{Ker} v$ et tel que (e_1, e_3) libre, par exemple $\boxed{e_1 = \begin{pmatrix} 5 \\ -1 \\ 0 \end{pmatrix}}$

(X) **Exo**

$$\begin{pmatrix} 0 & \cdots & \alpha_1 \\ & 0 \quad \diagup & \\ \alpha_n & & 0 \end{pmatrix} = u \qquad (\text{dans } \mathbb{C})$$

(e_i, e_{n-i+1}) = s.e.v. stable.

$\begin{cases} u(e_1) = \alpha_1 e_n \\ u(e_n) = \alpha_1 e_1 \end{cases}$ $\qquad u(e_i) = \alpha_{n-i+1}\, e_{n-i+1}$

Posons $E_i = (e_i, e_{n-i+1})$

$i = n-i+1 \Leftrightarrow 2i = n+1$

$\begin{cases} \text{Si } n \text{ pair, ils sont tous de dimension } 2 \\ \text{Si } n \text{ impair, il existe un seul } E_i \ (\text{pour } i = \frac{n+1}{2}) \text{ de dimension } 1, \text{ les autres étant de dim } 2. \end{cases}$

Si n pair $\quad E = \bigoplus_{1 \leq i \leq m} E_i \qquad u(E_i) \subset E_i$

Dans E_i, la matrice est $\begin{pmatrix} 0 & \alpha_i \\ \alpha_{n-i+1} & 0 \end{pmatrix}$.

O[illegible]appelle que :

u diagonalisable $\Leftrightarrow$ P_M a toutes ses racines simples.

$\Leftrightarrow$ $P_M = \text{ppcm}(P_{M_1}, \dots, P_{M_k})$ a toutes ses racines simples.

~~$E \simeq \bigoplus k[X]/(P_i)$~~

Th $\quad E = \bigoplus E_i \qquad u \in \text{End}(E) \,/\, u(E_i) \subset E_i$

P_M = polynôme minimale de u

P_{M_i} = " " de $u_i : E_i \to E_i$

Alors $P_M = \text{ppcm}(P_{M_i})_{1 \leq i \leq m}$

$$E_i = \bigoplus_j {}^{k[X]}/_{(P_{i_j})} \quad \text{et} \quad \operatorname{Ann}_{k[X]} E_i = P_{M_i}$$

Ainsi $E = \oplus N_i$ $\qquad N_i$ = sous-$k[X]$-modules. $= E_i$

$\operatorname{Ann} N_i = P_{M_i}$

oui : En effet : $x = (x_1, \dots, x_m)$

$\forall x \quad \lambda x = 0 \iff \begin{cases} \lambda x_i = 0 \\ \forall i \end{cases} \iff \forall i \; P_{M_i} \mid \lambda \iff \lambda$ mult. du $\operatorname{ppcm}_i(P_{M_i})$

En particulier, le $\operatorname{ppcm}_i(P_{M_i})$ convient.

Donc $\quad \operatorname{ppcm}_i(P_{M_i}) = P_M$

CQFD

$$\begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} = M_i$$

* Si $\alpha = \beta = 0 \qquad P_{M_i} = 0$
* Si α ou $\beta \neq 0 \qquad P_{M_i} = X^2 - \alpha\beta$

Montrons que

Pro | u diagonalisable $\iff$ u_i diagonalisable

$(\Leftarrow)$ trivial

$(\Rightarrow)$ u diagonalisable $\Rightarrow$ P_M n'a que des rac. simples.

$\Rightarrow \forall i \; P_{M_i}$ n'a que des racines simples.

$\Rightarrow u_i$ diagonalisable.

IMSP

Mathématiques

TD ALG 7

M1 UV Algèbre et Arithmétique

3.7.79

Feuille N°7

× 1°) Montrer que le pgcd des polynômes X^n-1 et X^m-1 est
X^d-1 où $d = \text{pgcd}(n, m)$

× 2°) Trouvez des matrices diagonales équivalentes aux matrices suivantes (le corps de base est $\mathbb{C}$)

$$\begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix} \quad \begin{pmatrix} X^2-1 & X+1 \\ X+1 & X^2+2X+1 \end{pmatrix} \quad \begin{pmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{pmatrix}$$

$$\begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \quad \text{etc....}$$

× 3°) Montrer que les matrices $\begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix}$ et $\begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix}$ sont semblables en calculant leurs invariants de similitude ; même question pour

$$\begin{pmatrix} 4 & 10 & -19 & 4 \\ 1 & 6 & -8 & 3 \\ 1 & 4 & -6 & 2 \\ 0 & -1 & 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 41 & -4 & -26 & -7 \\ 14 & -13 & -91 & -18 \\ 40 & -4 & -25 & -8 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4° Mettre sous la forme de Jordan les matrices suivantes (on calculera dans chaque cas le changement de base permettant de se ramener à la forme de Jordan) : $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$; $\begin{pmatrix} 12 & -6 & -2 \\ 18 & -9 & -3 \\ 18 & -9 & -3 \end{pmatrix}$;

$$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix} ; \begin{pmatrix} 0 & 0 & 0 & \cdots & n \\ \cdots & & & & \cdots \\ 0 & n & n-1 & \cdots & 2 \\ n & n-1 & n-2 & \cdots & 1 \end{pmatrix}$$

×5° Montrer que si $A = \begin{pmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & 0 \cdots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & & a & 1 \\ & & & & a \end{pmatrix}$ est une matrice de Jordan d'ordre n et si $f(x)$ est un polynôme à une variable, alors

$$f(A) = \begin{pmatrix} f(a) & f_1(a) & f_2(a) & \cdots & f_{n-1}(a) \\ 0 & f(a) & f_1(a) & \cdots & f_{n-2}(a) \\ \vdots & & & & \\ 0 & \cdots & & \cdots & f(a) \end{pmatrix}$$

où l'on pose $f_k(a) = \frac{1}{k!} f^{(k)}(a)$. Ceci suppose que le corps de base soit de caractéristique 0. Que se passe-t-il en caractéristique $p \neq 0$?

---

② $\begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & X^2 \end{pmatrix}$

$$\begin{pmatrix} X^2-1 & X+1 \\ X+1 & X^2+2X+1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} X+1 & 0 \\ 0 & P_2 \end{pmatrix} \quad (1)$$

où $(X+1)P_2 = (X^2-1)(X^2+2X+1) - (X+1)^2$

$(X+1)P_2 = (X+1)^2(X^2-2)$

d'où $P_2 = (X+1)(X^2-2)$

donc $(1) \rightsquigarrow \begin{pmatrix} X+1 & 0 \\ 0 & (X+1)(X^2-2) \end{pmatrix}$

$$\begin{pmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & X^2 & X \\ 0 & X & -X \\ 1 & X^2 & -X^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & X^2 & X \\ 0 & X & -X \\ 0 & 0 & -X^2-X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & -X \\ 0 & 0 & -X^2-X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^2+X \end{pmatrix}$$

$$\begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & X^2 & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X^3 & 1 \\ 0 & 0 & 0 & X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & X^4 \end{pmatrix}$$

Dessin

$$\underbrace{\begin{pmatrix} X & 1 & & 0 \\ & X & 1 & \\ & & \ddots & 1 \\ 0 & & & X \end{pmatrix}}_{n \text{ colonnes}} \Bigg]\ n \text{ lignes} \rightsquigarrow \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & X^n \end{pmatrix}$$

(3)

$$\begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix} = u \qquad \begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix} = v$$

$$u - XI = \begin{pmatrix} 3-X & 2 & -5 \\ 2 & 6-X & -10 \\ 1 & 2 & -3-X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & -X^2+4X-4 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

et

$$v - XI = \begin{pmatrix} 6-X & 20 & -34 \\ 6 & 32-X & -51 \\ 4 & 20 & -32-X \end{pmatrix} \rightsquigarrow \begin{pmatrix} -X & -12+X & \overbrace{17}^{\times \frac{1}{17}(X+1)} \\ 6 & 32-X & -51 \\ 4 & 20 & -32-X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & -12+X & 17 \\ -3(X+1)+6 & 32-X & -51 \\ \bigcirc +4 & 20 & -32-X \end{pmatrix} = \begin{pmatrix} 1 & X-12 & 17 \\ -3X+3 & -X+32 & -51 \\ -\frac{1}{17}(X^2+33X+32) & 20 & -X-32 \end{pmatrix}$$

$$-\frac{1}{17}(X+1)(X+32)$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 17 \\ -3X+3 & 3X^2-40X+68 & -51 \\ -\frac{1}{17}(X^2+33X+32) & & \end{pmatrix}$$

trop dur. Prenons une autre méthode

Calculons tous les mineurs d'ordre 2.

On trouve :

$$P_1P_2 = \text{pgcd}\Big((X-2)(X-36) ; 20(2-X) ; 9(X-2) ; 39(2-X) ; 20(2-X) ; (X-2)(X+2) ; 51(X-2) ; (X-2)(X+28) ; 6(2-X) \Big)$$

$P_1 = 1$. D'où $P_2 = X-2$.

Alors $\det(v - XI) = P_3(X-2) = -(X-2)^3 \Rightarrow P_3 = \pm(X-2)^2$

d'où

$$v - XI \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

Rappelons le théorème :

Th M = matrice à coefficients dans un corps K, et $n \times n$.

M et N semblables $\Leftrightarrow$ { $M-XI$ et $N-XI$ ont même diviseurs élémentaires dans $K[X]$ } $\Leftrightarrow$ { $M-XI$ et $N-XI$ équivalentes }

↓

ces div. él. sont appelés "invariants de similitude".

(4)

1)
$$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix} = u$$

$$\begin{pmatrix} -X & 1 & 0 \\ -4 & 4-X & 0 \\ -2 & 1 & 2-X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

$$E \simeq K[X]/(X-2) \oplus K[X]/(X-2)^2.$$

u semblable à
$$\left(\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 2 & 0 \\ 0 & 1 & 2 \end{array}\right)$$

chgt de base ? E_2 = vect. propre pour la vp 2.

$$\begin{cases} -2x + y = 0 \\ -4x + 2y = 0 \\ -2x + y = 0 \end{cases} \iff y = 2x \qquad \text{base } \left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} ; \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right)$$

e_1 e_3

On veut trouver e_2 / $f(e_2) = 2e_2 + e_3$

$e_2 \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ vérifie
$$\begin{cases} \beta = 2\alpha + 1 \\ -4\alpha + 4\beta = 2\beta + 2 \\ -2\alpha + \beta + 2\gamma = 2\gamma + 1 \end{cases}$$
d'où $e_2 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$

c) $\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1-X & -3 & 0 & 3 \\ -2 & -6-X & 0 & 13 \\ 0 & -3 & 1-X & 3 \\ -1 & -4 & 0 & 8-X \end{pmatrix}$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 2-X & \frac{1}{3}(X^2-3X+2) & X-1 \\ 0 & 4X-7 & \frac{1}{3}(-4X^2+11X-7) & X^2-5X+4 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & \frac{1}{3}(X-1)(X-2) & X-1 \\ 0 & 0 & -\frac{4}{3}(X-1)(X-\frac{7}{4}) & (X-1)(X-4) \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & X-1 & 0 \\ 0 & 0 & 0 & -\frac{1}{3}(X-1)^3 \end{pmatrix}$$

Invariants de similitudes $\quad 1,\ 1,\ X-1,\ (X-1)^3$

$$(E,u) \underset{\substack{K[X] \\ \text{moduls}}}{\simeq} \left(K[X]/(X-1) \oplus K[X]/(X-1)^3 \ , \ X\,\mathrm{id} \right)$$

$\dot{1} \to \dot{X}$

$\dot{(X-1)} \to \overline{X(X-1)}$

$\dot{(X-1)}^2 \to \overline{(X-1)}^2 X$

$$\begin{cases} \dot{X} = X-1+1 \\ X(X-1) = (X-1)^2 + X-1 \\ X(X-1)^2 = (X-1)^3 + (X-1)^2 \end{cases}$$

La matrice de Jordan de u est

$$\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

semblable à

$$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}$$

<u>Changement de base</u>

$E \underset{(\alpha)}{\simeq} K[X]/(X-1) \times K[X]/(X-1)^3$ Si $v = u - 1_E$

alors $v^3 = 0$ (cf. (α))

Retour au problème :

u diag $\Leftrightarrow$ u_i diag $\forall i$

$\Leftrightarrow \begin{cases} \text{Soit } \alpha_i = \alpha_{n-i+1} = 0 \\ \text{Soit } \alpha_i \alpha_{n-i+1} \neq 0 \end{cases} \quad \forall i$

Décomposition p primaire.

G ga fini

p premier $\quad G_p = \{x \in G \,/\, \exists \alpha \,/\, \omega(x) = p^\alpha\}$

G_p = sous-groupe de G est un p groupe.

C'est la p-composante de G $\doteq$ le plus grand p sgroupe de G.

Et $G = \prod_{p \in \mathcal{P}} G_p$

Preuve :

1) $\omega(x) = p^\alpha$

$\omega(y) = p^\beta$

$(xy)^{p^{\alpha+\beta}} = 1 \Rightarrow \omega(xy) \mid p^{\alpha+\beta} \Rightarrow xy \in G_p$

$G_p \neq \emptyset$ car $1 \in G_p$.

$\omega(x^{-1}) = \omega(x)$ ouï.

2) Gp est un p-groupe.

En effet : $\forall x \in G_p \quad \omega(x) = p^\alpha \Longrightarrow \# G_p = p^\beta$

Preuve :

$G_p = \{x_1, \dots, x_n\} \quad \prod_{1 \leq i \leq n} \langle x_i \rangle = \Gamma \quad \# \Gamma = p^\gamma$

$$\Gamma = \prod_{1 \leq i \leq n} \langle x_i \rangle \xrightarrow{\varphi} G_p$$

$$(y_1, \dots, y_n) \longmapsto y_1 \cdot \dots \cdot y_n$$

C'est un morphisme de groupe, surjectif.

$$\begin{array}{ccc} \Gamma & \xrightarrow{\varphi} & G_p \\ \pi \downarrow & \nearrow \sim & \\ \Gamma/H & & \end{array}$$

$H = \ker \varphi$

- $G_p \simeq \Gamma/H \Rightarrow \text{Card } G_p \mid \underbrace{\text{Card } \Gamma}_{p^\gamma} \Rightarrow \text{Card } G_p = p^\beta$ ceci.

3)

Important

G groupe cyclique d'ordre n $(\# G = n)$

Si $d \mid n$, $\exists !\, G_d$ sous-groupe de G tel que $\# G_d = d$

et $G_d = \{x \in G \,/\, dx = 0\}$

① $d = \delta(n,m) \Rightarrow X^d - 1 = \delta(X^n - 1, X^m - 1)$

Supposons que $m > n$

$(P) = (X^n - 1, X^m - 1) = (X^n - 1, X^{m-n} - 1)$; puisque

$$\begin{array}{r|l} X^m - 1 & X^n - 1 \\ -X^m + X^{m-n} & \overline{X^{m-n}} \\ \hline X^{m-n} - 1 & \end{array}$$

d'où

$(P) = (X^n - 1, X^m - 1) = (X^n - 1, X^r - 1)$ où $r = m - qn$, $0 \leq r < n$.

$(P) = (X^s - 1, X^r - 1)$ où s = reste de la division euclidienne de n par r

$$\begin{cases} m = qn + r \\ n = q_1 r + s \\ \vdots \\ a = bc + d \end{cases}$$
dernier reste non nul, $d = \delta(m,n)$

$c = \delta d$

d'où $(P) = (X^d - 1, X^c - 1)$ où $d \mid c$

Il est manifeste que $d \mid c \Rightarrow X^d - 1 \mid X^c - 1$

donc $(P) = (X^d - 1) \Rightarrow P = X^d - 1 = \Delta(X^n - 1, X^m - 1)$

2- méthode : On est dans $\mathbb{R}[X]$

On a $\begin{cases} (X^d - 1) f = X^n - 1 \\ (X^d - 1) g = X^m - 1 \end{cases}$

Montrons que $\delta(f, g) = 1$

$f = a \prod (X - a_i)^{\alpha_i}$ $a_i \in \mathbb{C}$

On a :

$\delta(f, g) = 1 \Leftrightarrow$ $\{$ f et g n'ont pas de racines dans $\mathbb{C}$ communes.

$(\Rightarrow)$ oui

(⇐) $D | f$ et $D | g$ et $D \in \mathbb{C}[X]$ f et g n'ont pas de racines complexes commune, donc $D = Cte = 1$ (Théorème de d'Alembert : "Tout polynôme de deg ≥ 1 admet au moins 1 racine)

Retournons à $\delta(f,g) = 1$:

Si $\alpha \in \mathbb{C}$ / $f(\alpha) = g(\alpha) = 0 \Rightarrow \begin{cases} \alpha^n - 1 = 0 \\ \alpha^m - 1 = 0 \end{cases}$ (1)

$\delta(n,m) = d \Longleftrightarrow \begin{cases} d | n \text{ et } d | m \\ \text{et} \\ d = un + vm \end{cases}$

donc $\alpha^d = (\alpha^n)^u (\alpha^m)^v = 1$

(1) $\Rightarrow \alpha^d - 1 = 0$

Ainsi $X^n - 1 = (X^d - 1) f$ admet α comme racine double.

Montrons que $X^n - 1$ n'admet pas de racines doubles :

$h = X^n - 1$ $\qquad \alpha^n = 1$

$h' = nX^{n-1}$

$h'(\alpha) = 0 \Rightarrow n\alpha^{n-1} = 0 \Rightarrow \alpha = 0$ (si le corps de caractéristique 0)

impossible.

Exo : k = corps fini $\exists f$ non constant $f \in k[X]$ qui n'a pas de racines.

Preuve :

$$f(X) = \prod_{i=1}^{n} (X - a_i) + 1 \quad \text{où } k = \{a_1, \dots, a_n\}$$

(5) Écrire $A = aI + J_n$ où $(J_n)^n = 0$

$$f(X) = \sum_{k \geq 0} \frac{(X-a)^k}{k!} f^{(k)}(a)$$ (Formule de Taylor pour les polynômes)

Appliqué en $A \in k[X]$

$$f(A) = f(a\,Id + J_n) = \sum_{k=0}^{\infty} \frac{J_n^k}{k!} f^{(k)}(a) = f(a) + \dots + J_n^{n-1} \frac{f^{(n-1)}(a)}{(n-1)!}$$

<u>Remarque</u> : On définit :

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = f(A) \in \mathcal{M}(n \times n)$$ car la série converge uniformément (c.à.d pour $\|\ \|_\infty$) et $\mathcal{M}(n \times n)$ = Banach.

- On trouve, par un m̂ calcul :

$$e^A = \begin{pmatrix} e^a & e^a & \cdots & \frac{e^a}{(n-1)!} \\ & \ddots & \ddots & \vdots \\ & & \ddots & e^a \\ 0 & & & e^a \end{pmatrix} = e^a \begin{pmatrix} 1 & \frac{1}{1!} & \frac{1}{2!} & \cdots & \frac{1}{(n-1)!} \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \ddots & \\ & & & \ddots & \frac{1}{1!} \\ 0 & & & & 1 \end{pmatrix}$$

- $$\boxed{\begin{array}{l} \det e^A = e^{na} \\ \operatorname{tr} e^A = na \end{array}}$$

<u>Remarque</u> : On a toujours $\boxed{\det e^A = e^{\operatorname{tr} A}}$ $\forall A$ matrice $\mathcal{M}(n \times n)$

En effet, A est décomposable en blocs de Jordan $\begin{pmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \\ & & & A_n \end{pmatrix}$

$$\begin{cases} \operatorname{tr} A = \sum \operatorname{tr} A_i \\ \det A = \prod \det A_i \end{cases}$$

On a $e^A = \begin{pmatrix} e^{A_1} & & \\ & \ddots & \\ & & e^{A_n} \end{pmatrix} \Rightarrow \det e^A = \prod \det e^{A_i} = \prod e^{\operatorname{tr} A_i}$

$$= e^{\sum \operatorname{tr} A_i} = e^{\operatorname{tr} A}$$ CQFD

IMSP

M1 Algèbre et Arithmétique

28.3.79

Feuille N° 8

×1° Quels sont les polynômes irréductibles de degrés 2 et 3 à coefficients dans $\mathbb{F}_2$? Donner des tables de multiplication de $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$.

×2° Soit A une $\mathbb{R}$-algèbre de dimension 2 (i.e un anneau muni d'une structure de $\mathbb{R}$-espace vectoriel dont la loi de groupe est celle de l'anneau). Soit $\{1, e\}$ une base de A. Montrer qu'il existe un polynôme $f \in \mathbb{R}[X]$ de degré 2 vérifiant $f(e) = 0$. En déduire que A est isomorphe à l'une des trois algèbres suivantes : $\mathbb{R}\times\mathbb{R}$ avec la loi $(x, y)(x', y') = (xx', yy')$, $\mathbb{R}[X]/(X^2)$ (nombres duaux, ou développements limités au deuxième ordre), $\mathbb{C}$.

×3° Soit $f \in \mathbb{Q}[X]$ le polynôme $X^3 - 2$.

a) montrer que f est irréductible.

b) montrer que le plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt[3]{2}$ est le corps de rupture de f ; on le note $\mathbb{Q}(\sqrt[3]{2})$. Écrire explicitement les éléments de $\mathbb{Q}(\sqrt[3]{2})$; calculer $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$

c) Quel est le corps de décomposition K de f ? a-t-on

$k = \mathbb{Q}(\sqrt[3]{2})$? Calculer $\dim_{\mathbb{Q}} k$.

× 4° Soient L un corps fini, k un sous-corps de L, ξ un générateur de $(L^*, \times)$.

a) montrer que le plus petit sous-corps de L contenant k et ξ est L

b) On définit $\varphi : k[X] \to L$ par $\varphi(f) = f(\xi)$. Alors

i) φ est un morphisme surjectif d'anneaux.

ii) il existe un polynôme irréductible $f \in k[X]$ vérifiant $f(\xi) = 0$ et $L \simeq k[X]/f\,k[X]$

c) Montrer que si k est un corps fini, n un entier au moins égal à 2, il existe un polynôme irréductible de degré n dans $k[X]$.

5° Soit un nombre premier p et soit un corps $\mathbb{F}_q$ de caractéristique p, $n > 0$ un entier premier avec p. Soit k le corps des ~~décomposition~~ racines de $X^n - 1$ sur $\mathbb{F}_q$.

a) Montrer que $n \mid (\# k - 1)$

b) Montrer que $k = \mathbb{F}_{q^m}$ où $m = \min\{\lambda \in \mathbb{N}^* \mid n \mid q^{\lambda} - 1\}$

c) Conclure que si p est premier, si $\alpha \in \mathbb{N}^*$, $n \in \mathbb{N}^*$ et $(p, n) = 1$, il existe $m \in \mathbb{N}^*$ vérifiant $n \mid p^{\alpha m} - 1$. Que se passe-t-il si p n'est pas premier ?

28.3.79

Page de (de Feuilles 8)

(1) $p \in \mathcal{P}$ $n \in \mathbb{N}^*$

$\mathbb{F}_{p^n}$ = corps à p^n éléments

lemme (K = corps) — important

$2 \leq \deg f \leq 3$ f irréductible dans K $\Leftrightarrow$ n'a pas de racine dans K.

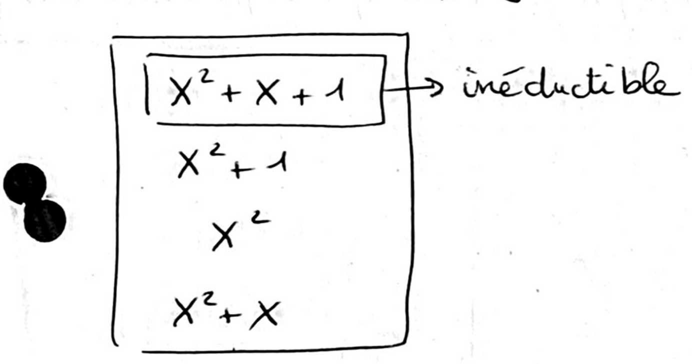
Preuve : f non irréductible $\Leftrightarrow$ $f = gh$ $\begin{cases} \deg h \geq 1 \\ \deg g \geq 1 \end{cases}$

$\begin{cases} \text{et } \deg f = 2 \Rightarrow \deg h = 1 \ \deg g = 1 \Rightarrow f \text{ possède une racine.} \\ \text{et } \deg f = 3 \Rightarrow h \text{ ou } g \text{ est de degré } 1 \Rightarrow f \text{ possède une racine.} \end{cases}$

L'équivalence en résulte.

1°/ $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

$X^2 + aX + b$ 4 polynômes de degré 2.



Si le polynôme est de degré 3 :

$P = X^3 + aX^2 + bX + c$ 8 choix

P réductible $\Leftrightarrow$ P admet une racine (0 ou 1)

Si cette racine est 0, alors $c = 0$, $P = X^3 + aX^2 + bX$ soit 4 choix possibles.

Si cette racine est 1, $1 + a + b + c = 0 \Leftrightarrow (a,b,c) = (0,1,0)$, $(1,0,0)$ } ici $c = 0$.
$(0,0,1)$
$(1,1,1)$

Deux triplets (0,1,0) et (1,0,0) sont à écarter puisqu'ils ont déjà été comptés (cf. c=0).
En conclusion, il y a 6 réductibles sur 8.

En conclusion :

P de deg 2	1 irréductible sur 4	(dans $\mathbb{F}_2$)
P de deg 3	2 " sur 8	

2)

On rappelle que :

$f \in k[X]$ f irréductible $\Leftrightarrow$ $k[X]/(f)$ corps [(f) maximal]

(corps de rupture de k)

Si k est fini, on a $\# \text{Card}\left(k[X]/(f) \right) = (\text{Card } k)^{\deg f}$

et que : tous les corps $\mathbb{F}_q$ à q éléments sont isomorphes, en tant que corps, entre eux.

X^2+X+1 est irréductible dans $\mathbb{F}_2$

Ainsi

$$\mathbb{F}_2[X]/(X^2+X+1) = \{\dot{0}, \dot{1}, \dot{X}, \dot{X}^2\}$$

ce sont bien 4 éléments distincts.

On a $\dot{X}.\dot{X}^2 = X^3 = X(X^2+X+1) - X^2 - X$
$= + X^2 + X = 1$

Tables de multiplication de $\mathbb{F}_8$

On fait de même ;

$\mathbb{F}_2[X]/_{(X^3+X+1)} = \{ \dot{0}, \dot{1}, \dot{X}, \dot{X}^2, \dot{X}^3, \dot{X}^4, \dot{X}^5, \dot{X}^6 \}$

tous distincts

(possède $2^3 = 8$ éléments)

On : $\dot{X}^7 = \dot{X}^6 . \dot{X} = \dot{1}$

On connaît la table de multiplication du corps $\mathbb{F}_2[X]/_{(X^3+X+1)}$ à 8 éléments.

$\mathbb{F}_9$

$f \in \mathbb{F}_3[X]$ $\deg f = 2$ $X^2 + aX + b$ $a \in \{-1, 0, 1\}$
$b \in \{-1, 1\}$

On en choisit un qui soit irréductible : On a le choix entre

$\boxed{X^2+X+1}$

$\boxed{X^2+1}$ (et les mêmes multipliés par (-1))

$\boxed{X^2+X-1}$

$\boxed{X^2-X-1}$

D'où $\mathbb{F}_9 \underset{\text{corps}}{\simeq} \mathbb{F}_3[X]/_{(X^2+1)}$

② $A = \mathbb{R}$-algèbre de dimension 2.

$$\begin{cases} (A,+,.) \text{ ev} \\ (A,+,\times) \text{ anneau} \\ \lambda(x\times y) = (\lambda x)\times y = x\times(\lambda y) \end{cases}$$

Par exemple $\mathbb{C}$, $\mathbb{R}[X]/(X^2)$ = "nombres duaux" = $\{a+b\varepsilon, \text{ où } \varepsilon^2=1\}$, $\mathbb{R}\times\mathbb{R}$

<u>Exercice</u> ; $B = C^{\infty}_{\mathbb{R}}[-1,1]$

$I = \{f \in B \,/\, f(0) = \dots = f^{(n)}(0) = 0\}$ idéal de B

$(B, I) \Leftrightarrow (\mathbb{R}[X], (X^{n+1}))$

On peut dire que $B/I \simeq \mathbb{R}[X]/(X^{n+1})$

En effet :

$B \xrightarrow{\text{morphisme surj d'anneaux}} \mathbb{R}[X]/(X^{n+1})$

$f \longmapsto$ classe de $\left(\sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} X^k\right)$

$\downarrow$

$B/I \nearrow$ $\sim$ isomorphisme.

<u>A de base $\{1, e\}$</u>

Trouver f / $\deg f = 2$ / $f(e) = 0$.

Prenons $f(X) = X^2 + bX + c$

$f(e) = 0 \Leftrightarrow e^2 + be + c = 0$

$\Leftrightarrow e^2 = -c - be$

Ainsi : $e^2 = a.1 + be$ $\quad a, b \in \mathbb{R}$

$f(X) = X^2 - bX - a \Rightarrow f(e) = 0$

(3) Considérons

$$\mathbb{R}[X] \xrightarrow{\varphi} A$$
$$g \longmapsto g(e)$$

φ = homomorphisme d'algèbre surjectif de noyau $\ker\varphi = \{f\}$

En effet $\forall a \in A$ $\quad a = \alpha.1 + \beta e = (\alpha + \beta X)(e)$

On a $(f) \subset \ker\varphi$ puisque $f(e) = 0$.

Montrons que $(f) = \ker\varphi$.

<u>lemme:</u> $\left.\begin{array}{l} g \in \mathbb{R}[X] \setminus \{0\} \\ \deg g = 0 \text{ ou } 1 \end{array}\right\} \Rightarrow g(e) \neq 0$ (facile)

d'où $\deg f = \inf\{\deg m \,/\, m \in \ker\varphi\} \geq 2$ et $f \in \ker\varphi$ $\deg f = 2$.

Donc $\ker\varphi = (f)$. oui

Tout cela pour:

$$\mathbb{R}[X] \xrightarrow{\varphi} A$$
$$g \longmapsto g(e)$$

$\pi \downarrow$ $\quad \mathbb{R}[X]/(f) \nearrow$ $\sim$ d'algèbre

Ainsi : $A \underset{alg}{\simeq} \mathbb{R}[X]/(f)$

De 3 choses l'une :

1) <u>f n'a pas de racines.</u>

$f(X) = (X+\alpha)^2 + \beta^2 \qquad \alpha, \beta \in \mathbb{R}$

$$\mathbb{R}[X]/_{(\beta)} \xrightarrow[\sim]{\dot{\varphi}} \mathbb{C}$$

$\uparrow$

$\mathbb{R}[X] \longrightarrow$

$g \longmapsto g(\beta i - \alpha)$ } car $\left(\dfrac{\dot{\overline{X+\alpha}}}{\beta}\right)^2 + \dot{1} = \dot{0}$

donc $\varphi\left(\dfrac{X+\alpha}{\beta}\right) = i$

φ = homomorphisme d'algèbre.
(c'est le complexe "polynome en un point")

$\text{Ker}\,\varphi = \{ g \in \mathbb{R}[X] / g(\beta i - \alpha) = 0 \}$

Si $g(\beta i - \alpha) = 0$, alors $g(-\beta i - \alpha) = 0$, et donc

$$(X - \beta i + \alpha)(X + \beta i + \alpha) \mid g$$

$$\Updownarrow$$

$$(X+\alpha)^2 + \beta^2 \mid g$$

$$\Updownarrow$$

$$\dot{g} = \dot{0} \text{ dans } \mathbb{R}[X]/_{(\beta)}$$

Donc $\text{Ker}\,\varphi = (\beta)$.

Enfin, φ est surjective car $\begin{cases} \varphi(1) = 1 \\ \varphi\left(\dfrac{X+\alpha}{\beta}\right) = i \end{cases}$

En conclusion $A \underset{alg}{\simeq} \mathbb{R}[X]/_{(\beta)} \underset{alg}{\simeq} \mathbb{C}$

2) $\underline{\Delta = 0}$

$$\mathbb{R}[X]/_{(\beta)} \xrightarrow[\sim]{\bar{\varphi}} \mathbb{R}[X]/_{(X^2)}$$

$\uparrow$

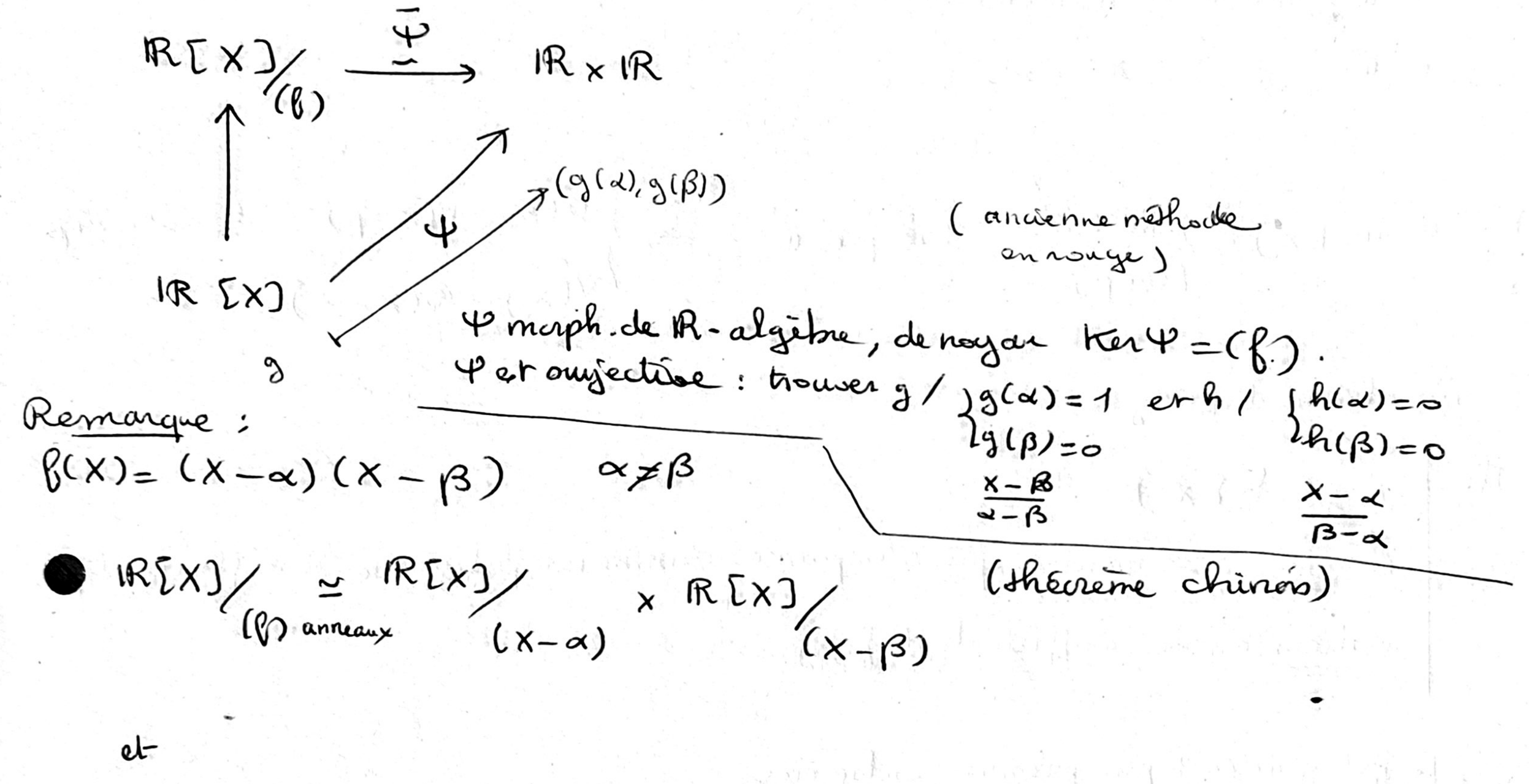
$\mathbb{R}[X] \longrightarrow$

$g \overset{\varphi}{\longmapsto} \dot{\overline{g(X+\alpha)}}$

(puisque $(X-\alpha)^2 \xrightarrow{\varphi} 0$)

~~donc $\varphi(X) = (X-\alpha)$~~

3) 2 racines distinctes



Ψ morph. de $\mathbb{R}$-algèbre, de noyau $\operatorname{Ker}\Psi = (f)$.
Ψ est surjective : trouver g / $\begin{cases} g(\alpha)=1 \\ g(\beta)=0 \end{cases}$ et h / $\begin{cases} h(\alpha)=0 \\ h(\beta)=0 \end{cases}$

$\dfrac{X-\beta}{\alpha-\beta}$ $\qquad$ $\dfrac{X-\alpha}{\beta-\alpha}$

(théorème chinois)

Remarque :
$f(X) = (X-\alpha)(X-\beta)$ $\qquad \alpha \neq \beta$

- $\mathbb{R}[X]/(f) \underset{\text{anneaux}}{\simeq} \mathbb{R}[X]/(X-\alpha) \times \mathbb{R}[X]/(X-\beta)$

et

$\mathbb{R}[X]/(X-\alpha) \simeq \mathbb{R}$

$\dot{h} \longmapsto h(\alpha)$

Mais on avait seulement un morphisme d'anneaux. Il y a encore à travailler.

Conclusion : Il n'y a que 3 structures de $\mathbb{R}$-algèbre de dimension 2, à isomorphisme près, bien sûr.

$A \underset{\text{alg.}}{\simeq}$

⊗ Remarque :

$\alpha \in \mathbb{C}$ racine de $X^3 + X + 1 = 0$

$\beta \in \mathbb{C}$ " $X^2 + X - 3 = 0$

$P, Q \in \mathbb{Q}[X]$ $\begin{cases} P(\alpha) = 0 \\ Q(\beta) = 0 \end{cases}$ $\alpha, \beta \in \mathbb{C}$ $\Rightarrow$ $\begin{cases} U(X) = P(X - \beta) & \text{de racine } \alpha + \beta \\ V(X) = Q(X - \alpha) & " \end{cases}$

Résultant de f et g

Th | $f, g \in k[X]$
Res (f, g) = nombre qui s'exprime comme un polynôme à coefficients entiers en les coefficients de f et g

Pro | f et g ne sont pas premiers entre eux
$\Updownarrow$
$\text{Res}(f, g) = 0$

{ coefficients de U = polyn. en β à coefficients dans $\mathbb{Q}$

On prendra plutôt

$$\begin{cases} U(X) = P\left(X + \frac{\alpha + \beta}{2}\right) & U\left(\frac{\alpha - \beta}{2}\right) = 0 \\ V(X) = Q\left(-X + \frac{\alpha + \beta}{2}\right) & V\left(\frac{\alpha - \beta}{2}\right) = 0 \end{cases}$$

On calcule le résultant de U et V, qui est nul. (cf. Th.) et c'est un polynôme en $\alpha + \beta$ à coeff. entiers.

X

Résultant

$$\begin{cases} d = \deg P \\ e = \deg Q \end{cases} \qquad S_k = \{ f \in K[X] \ / \ \deg f < k \}$$

$$S_d \oplus S_e \xrightarrow{\ \Phi\ } S_{d+e}$$
$$(u, v) \longrightarrow uQ + vP$$

Φ est linéaire.

Φ surjective $\Rightarrow \exists u, v \ / \ uP + vQ = 1 \Rightarrow \delta(P, Q) = 1$.

$\delta(P, Q) = 1 \Rightarrow$ Φ injective car $uQ = -vP \Rightarrow P | u \Rightarrow u = 0 \Rightarrow v = 0$.
$\Rightarrow$ Φ bijective (espaces ont $\hat{m}$ dimension)

Ainsi : Φ isomorphisme $\Leftrightarrow \delta(P, Q) = 1$

$$\begin{cases} S_d \oplus S_e \text{ de base } (1,0)\ (X,0) \dots (X^{d-1},0)\ (0,1) \dots (0,X^{e-1}) \\ S_{d+e} \text{ de base } 1 \ X \dots X^{d+e-1} \end{cases}$$

Exprimons Φ dans ces bases :

$$\begin{cases} P = \sum_{i=0}^{d} a_i X^i \\ Q = \sum_{j=0}^{e} b_j X^j \end{cases}$$

d colonnes

$$\text{mat } \Phi = \begin{pmatrix} b_0 & 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 \\ b_1 & b_0 & & \vdots & a_1 & a_0 & & \vdots \\ \vdots & b_1 & & 0 & \vdots & a_1 & & 0 \\ b_e & b_{e-1} & & b_0 & a_{d-1} & \vdots & & a_0 \\ 0 & b_e & & b_1 & a_d & a_{d-1} & & \vdots \\ \vdots & 0 & & \vdots & 0 & a_d & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & b_e & 0 & \cdots & & a_d \end{pmatrix}$$

d − 1 zéros

Application : (cf. feuille 4 de ce TD).

$$\begin{cases} P = X^3 + X + 1 & P(\alpha) = 0 \\ Q = X^2 + X - 3 & P(\beta) = 0 \end{cases}$$

On a :

$$\text{Res}\Big(\underbrace{P\big(X + \tfrac{\alpha+\beta}{2}\big)}_{U},\ \underbrace{Q\big(-X + \tfrac{\alpha+\beta}{2}\big)}_{V}\Big) = 0$$

car $\delta(U, V) \neq 0$.

$u = \alpha + \beta$

$$P\left(X + \frac{u}{2}\right) = X^3 + 3X^2\frac{u}{2} + 3X\frac{u^2}{4} + \frac{u^3}{8} + X + \frac{u}{2} + 1$$

$$= \frac{1}{8}\left[8X^3 + 12uX^2 + (6u^2 + 8)X + u^3 + 4u + 8\right]$$

ne servira à rien pour l'annulation du résultant.

$$Q\left(-X + \frac{u}{2}\right) = X^2 + \frac{u^2}{4} - uX - X + \frac{u}{2} - 3$$

$$Q\left(-X + \frac{u}{2}\right) = \frac{1}{4}\left[4X^2 - 4(u+1)X + u^2 + 2u - 12\right]$$

$$\det\begin{pmatrix} 8 + 4u + u^3 & 0 & -12 + 2u + u^2 & 0 & 0 \\ 8 + 6u^2 & 8 + 4u + u^3 & -4(u+1) & -12 + 2u + u^2 & 0 \\ 12u & 8 + 6u^2 & 4 & -4(u+1) & -12 + 2u + u^2 \\ 8 & 12u & 0 & 4 & -4(u+1) \\ 0 & 8 & 0 & 0 & 4 \end{pmatrix}$$

(3) $f \in \mathbb{Q}[X]$ $\quad f = X^3 - 2$

a) $\frac{p^3}{q^3} - 2 = 0 \Leftrightarrow p^3 - 2q^3 = 0 \Rightarrow q \mid p$ (car $\delta(p,q)=1$)

donc $q = 1$ (on peut prendre $q > 0$)

Alors $p^3 = 2 \Rightarrow p = \pm 1$ ou ± 2. Aucune de ces valeurs ne convient.

Donc : f n'admet pas de racines rationnelles.

Le lemme suivant permet de conclure :

<u>Lemme</u> : K = corps.

$P \in K[X]$ / $\deg P = 2$ ou 3 (<u>important</u>)

Alors P irréductible sur $K[X] \Leftrightarrow \nexists x \in K$ / $P(x) = 0$

b) $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3-2)$

en corps.

$\mathbb{Q}(\sqrt[3]{2})$ est un espace vectoriel de dimension 3 sur $\mathbb{Q}$, de base $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$

$$\mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \;/\; a,b,c \in \mathbb{Q} \}$$

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$$

c)

<u>A-t'on $K = \mathbb{Q}(\sqrt[3]{2})$</u>

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + X\sqrt[3]{2} + 2^{\frac{2}{3}}) \quad \text{dans } \mathbb{Q}(\sqrt[3]{2})[X]$$

Le polynôme $(X^2 + \sqrt[3]{2}X + 2^{\frac{2}{3}})$ est-t'il irréductible dans $\mathbb{Q}(\sqrt[3]{2})[X]$

S'il ne l'est pas, il existe $x = a + b\sqrt[3]{2} + c\sqrt[3]{2^2}$ racine de ce polynôme :

$$(a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}})^2 + 2^{\frac{1}{3}}(a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}}) + 2^{\frac{2}{3}} = 0 \qquad a,b,c \in \mathbb{Q}$$

d'où

$$a^2+4bc+2c+2^{\frac{1}{3}}(a+2ab+2c^2)+2^{\frac{2}{3}}(1+2ac+b^2+b)=0$$

$$\begin{cases} a^2+4bc+2c=0 & (1) \\ a+2ab+2c^2=0 & (2) \\ 1+2ac+b+b^2=0 & (3) \end{cases}$$

$(3) \Rightarrow 2c(1+2b)=-a^2 \Rightarrow 4c^2(1+2b)^2=a^4$

or $(2) \Rightarrow 2c^2=-a(1+2b)$ d'où $a[a^3+2(1+2b)^3]=0$

$a\neq 0$ car $a=0 \Rightarrow c=0 \Rightarrow b^2+b+1=0$ et $b\in\mathbb{Q}$, faux.

donc $a\neq 0 \Rightarrow a^3+2(1+2b)^3=0 \Rightarrow \frac{a^3}{(1+2b)^3}+2=0$

impossible sur $\mathbb{Q}$ car X^3+2 est irréductible sur $\mathbb{Q}$

Donc $X^2+2^{\frac{1}{3}}X+2^{\frac{2}{3}}$ est irréductible sur $\mathbb{Q}(\alpha)$ $\quad \alpha=\sqrt[3]{2}$

Conclusion :

$$\boxed{K\neq\mathbb{Q}(\sqrt[3]{2})}$$

dimension 3

$\dim_{\mathbb{Q}} K$?

$F=\mathbb{Q}(\alpha)[X]/(X^2+2^{\frac{1}{3}}X+2^{\frac{2}{3}})$ = corps de rupture du polynôme $X^2+2^{\frac{1}{3}}X+2^{\frac{2}{3}}$ (par ex. $\beta=j\alpha$)

$\dim_{\mathbb{Q}(\alpha)} F=2$

$\forall f\in F \quad f=a+b\dot{X} \quad a,b\in\mathbb{Q}(\alpha)$

$\dot{X}\doteq\beta$

$\forall f\in F \quad f=(a_1+a_2\alpha+a_3\alpha)+(b_1+b_2\alpha+b_3\alpha)\beta \quad \beta=j\alpha$

$$\beta \in F \Leftrightarrow \beta = a_1 + a_2\alpha + a_3\alpha + b_1\beta + b_2\alpha\beta + b\alpha^2\beta$$
~~$a_1 + a_2\alpha + b_1\beta + b_2\alpha\beta$~~ $\qquad (\alpha\beta = j\alpha^2)$

$a_i, b_i \in \mathbb{Q}$

$$\dim_{\mathbb{Q}} F = [F ; \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) ; \mathbb{Q}]$$

$$\dim_{\mathbb{Q}} F = 2 \times 3 = 6$$

~~dem~~

On a $F = K$ = corps des racines de f

- Car, si α, β, γ sont les 3 racines de f dans $\mathbb{C}$,

$$F = \mathbb{Q}(\alpha, \beta) \underset{\text{évident}}{=} \mathbb{Q}(\alpha)(\beta)$$

puisque $\mathbb{Q}(\alpha)(\beta) \simeq \mathbb{Q}(\alpha)[X] / (X^2 + 2^{\frac{1}{3}}X + 2^{\frac{2}{3}})$

En effet, $f(X) = X^3 - 2 = \underbrace{(X-\alpha)(X-\beta)}_{\in F[X]} Q(X) \qquad \deg Q = 1$

- La dernière racine appartient donc à F.

F est donc un corps de factorisation de $f(X)$. Montrons que c'est le corps des racines de $f(X)$, c.à.d que

si Σ = corps tel que $\begin{cases} \mathbb{Q} \subset \Sigma \subset F \\ \Sigma \text{ de factorisation de } f(X) \end{cases}$ alors $\Sigma = F$

$$\alpha, \beta \in \Sigma \text{ et } \mathbb{Q} \subset \Sigma \Rightarrow \underbrace{\mathbb{Q}(\alpha, \beta)}_{F} \subset \Sigma \Rightarrow F \subset \Sigma$$

Donc $F = K$ est de dimension 6 sur $\mathbb{Q}$

Corps de rupture

Rappels : le plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt[3]{2}$ est le corps de rupture de f

Déterminer $\mathbb{Q}(\sqrt[3]{2})$

On rappelle le diagramme

$$\begin{array}{ccc} \mathbb{Q}[X] & \xrightarrow{\varphi} & \mathbb{Q}(\sqrt[3]{2}) \\ P & \longmapsto & P(\sqrt[3]{2}) \\ \pi \downarrow & \nearrow & \\ \mathbb{Q}[X]/(X^3-1) & & \end{array}$$

$\bar{\varphi}$ est un isomorphisme d'algèbre.

donc $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \dim_{\mathbb{Q}} \mathbb{Q}[X]/(X^3-1) = 3$

et ~~…~~ $(1, X, X^2)$ est une base de $\mathbb{Q}[X]/(X^3-1)$. Donc $(\bar{\varphi}(1), \bar{\varphi}(X), \bar{\varphi}(X^2))$ est une base de $\mathbb{Q}(\sqrt[3]{2})$ comme espace vectoriel sur $\mathbb{Q}$.

$$\begin{cases} \bar{\varphi}(1) = \varphi(1) = 1 \\ \bar{\varphi}(X) = \varphi(X) = \sqrt[3]{2} \\ \bar{\varphi}(X^2) = \varphi(X^2) = (\sqrt[2]{2})^2 \end{cases}$$

d'où $\boxed{\mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \ / \ a, b, c \in \mathbb{Q} \}}$

Remarque : $Gal(\mathbb{Q}(\alpha, j\alpha)/\mathbb{Q}) = Aut(\underbrace{\mathbb{Q}(\alpha, j\alpha)}_{K})$

Soit $\sigma \in Aut(K)$

Si $x \in K$ $\lambda \in \mathbb{Q}$ $\sigma(\lambda x) = \lambda \sigma(x)$

Si ξ est racine de $f \in \mathbb{Q}[X]$, alors $\sigma(\xi)$ aussi. En effet, si $f(X) = \sum a_k X^k$

$f(\xi) = \sum a_k \xi^k \Rightarrow f(\sigma(\xi)) = \sum a_k (\sigma(\xi))^k = \sigma(\sum a_k \xi^k) = \sigma(0) = 0$

car σ est un morphisme de corps ($\Rightarrow \sigma$ est $\mathbb{Q}$-linéaire)

Posons : $\Phi : Gal(K) \longrightarrow \mathcal{S}\{\alpha, \beta, \gamma\}$ α, β, γ racines de f

$\sigma \longmapsto \sigma|_{\{\alpha,\beta,\gamma\}}$

- Alors Φ est injective : En effet, si $\sigma|_{\{\alpha,\beta,\gamma\}} = \sigma'|_{\{\alpha,\beta,\gamma\}}$

La base $(1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta)$ est transformée en $\mathcal{B}'$ par σ et par σ' morphismes de corps. Donc $\sigma = \sigma' \Rightarrow \Phi$ est injective.

On peut écrire

$$\boxed{\Phi : Gal(K) \hookrightarrow \mathcal{S}\{\alpha, \beta, \gamma\}}$$

↑ (Résultat général)

- *En particulier*, si $f = X^3 - 2$, montrons que Φ est surjective.

$$\begin{cases} \alpha = \sqrt[3]{2} \\ \beta = j\alpha \\ \gamma = j^2\alpha \Rightarrow \gamma = \beta^2\alpha^{-1} \end{cases}$$

Soit $\theta \in \mathcal{S}\{\alpha, \beta, \gamma\}$, alors considérons $\sigma \in Gal(K)$ défini par :

$$\sigma : \begin{array}{cccccc} 1 & \alpha & \alpha^2 & \beta & \alpha\beta & \alpha^2\beta \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & \theta(\alpha) & \theta(\alpha)^2 & \theta(\beta) & \theta(\alpha)\theta(\beta) & \theta(\alpha)^2\theta(\beta) \end{array}$$

σ est une ~~autom~~ application $\mathbb{Q}$-linéaire. En fait, c'est un automorphisme

des corps $\mathbb{Q}(\alpha, \alpha_j)$: pour le montrer, nous aurions affaire à des calculs compliqués.

(4) a) trivial

b) Facile (le faire !)

<u>Remarque</u> :

$I \subset A$ A anneau

<u>I premier</u> $\Leftrightarrow$ A/I intègre $\Leftrightarrow \forall x, y \in A \quad xy \in I \Rightarrow x$ ou $y \in I$

Ainsi : <u>I maximal</u> $\Rightarrow$ I premier

$\Updownarrow$ $\nearrow$

A/I = corps

<u>I principal</u> $\Leftrightarrow$ $\exists a \in A / I = (a)$ ~~I intègre et ∀ J idéal J ⊂ I~~

Pro | ~~Si A est principal, alors I premier ⇒ I maximal~~

Pro | Soit A un anneau principal
Si I premier dans A, ~~alors~~ ssi $I = (p)$ où $p =$ ~~premier~~ irréductible

Def | $p \in A$ est dit ~~pr~~ irréductible ssi $\quad p = uv \quad u, v \in A \Rightarrow u$ ou $v \in A^*$.

~~Pas~~

Preuve de la Pro :

($\Leftarrow$) $\quad p = uv \Rightarrow p | uv \Rightarrow p | u$ ou $p | v$ ~~⇒ p~~

Par exemple $p | u \Leftrightarrow u = \lambda p \Rightarrow 1 = \lambda v \Rightarrow v \in A^*$ ~~⇔~~

c)

$\left.\begin{array}{l} p \text{ premier} \\ n \text{ entier} \end{array}\right\} \Rightarrow \exists!$ corps à p^n éléments $\mathbb{F}_{p^n}$

1) $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m}$ (morphisme de corps) alors $q = p$ $n \leq m$

$(\mathbb{F}_{p^n}^*, \times) \underset{\text{groupe}}{\hookrightarrow} (\mathbb{F}_{p^m}^*, \times) \Rightarrow$ (Lagrange) $p^n - 1 \mid p^m - 1 \Rightarrow n \mid m$

En conclusion

- $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m} \Rightarrow$ $\boxed{p = q \text{ et } n \mid m}$

2) $\mathbb{F}_{p^m}$ est muni d'une structure de $\mathbb{F}_{p^n}$-ev si $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m}$ ~~q~~ $n \leq m$.
$\mathbb{F}_{p^m}$ est de dimension finie, donc :

$$\exists d \in \mathbb{N} \ / \quad \# \mathbb{F}_{p^m} \simeq (\mathbb{F}_{p^n})^d$$

-
$$p^m = p^{nd}$$
$$\Downarrow$$
$$m = nd$$
$$\Downarrow$$
$$n \mid m$$

(<u>Remarque</u> : la démonstration ~~et~~ faite au 1) ~~est moins~~ suppose moins de connaissances)

. <u>Réciproquement</u> ? voir (*1)

On rappelle que : k corps $f \in k[X]$

$K \supset k$ est corps des racines $\Longleftrightarrow \left\{ \begin{array}{l} f \text{ se décompose et} \\ K = \text{le plus petit sous-corps} \\ \text{contenant les racines de } f \end{array} \right.$

(*2)

Pro | Si il existe un corps L de décomposition de $f \in k[X]$
Alors il existe un morphisme injectif $K \hookrightarrow L$, c-à.d

Preuve :

$\xi_1, \dots, \xi_n$ = racines de f dans L

Considérons $k(\xi_1, \dots, \xi_n) = K'$. C'est un corps des racines de $f \in k[X]$

D'après l'unicité (à isomorphisme près) du corps des racines :

$$\begin{array}{ccc} K & \xrightarrow{\sim} & K' \\ & & \downarrow \\ & & L \end{array}$$

d'où $K \hookrightarrow L$ (morph. inj. de corps) CQFD

On rappelle que $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n}$ = corps des racines de $X^{p^n} - X \in \mathbb{F}_p[X]$

(*1) Hypothèse : $m = nd$

$$\# \{a \in \mathbb{F}_{p^m} \ / \ g(a) = 0\} = \# \{a \in \mathbb{F}_{p^m} \ / \ a^{p^n} = a\}$$

$$= \# \{a \in \mathbb{F}_{p^m}^* \ / \ a^{p^n - 1} = 1\} + 1$$

Comme $n | m \Rightarrow p^n - 1 | p^m - 1$, donc $\# \{a \in \underbrace{\mathbb{F}_{p^m}^*}_{\text{cyclique}} \ / \ a^{p^n - 1} = 1\} = p^n - 1$

d'où

$$\# \{a \in \mathbb{F}_{p^m} \ / \ g(a) = 0) = p^n$$

ce qui prouve que g possède toutes ses racines dans $\mathbb{F}_{p^m}$. $\mathbb{F}_{p^m}$ est un corps de décomposition de g. D'après le théorème (*2), $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$

Ce qui prouve que $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$.

d'où le théorème :

Th $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m} \iff n \mid m$

$K = \mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^{an}} = L$ où $[L ; \mathbb{F}_{p^a}] = n$

D'après le a) et le b) $\exists f$ irréductible de degré n sur $\mathbb{F}_{p^a}[X] = K[X]$

●

(5)

Remarque : exo

$\forall x \not\equiv 0$ $[2]$ et $[5]$ $\exists n$ tel que $x \mid \underbrace{99\ldots9}_{n \text{ neufs}}$.

c'est une conséquence de l'exercice (5).

●

p premier car$(\mathbb{F}_q) = p$ $q = p^m$.

$\delta(n, p) = 1$ K = corps des racines de $X^n - 1 \in \mathbb{F}_q[X]$

a) $n \mid (\# K - 1)$

$\{x \in K \,/\, x^n = 1\} \subset K^*$

$\{x \in K \,/\, x^n = 1\}$ est un sous-groupe du groupe multiplicatif $(K^*, \times)$

Cherchons $\# \{x \in K / x^n = 1\}$. Tous les éléments de $\{x \in K / x^n = 1\}$ sont distincts car le polynome $X^n - 1$ admet pour dérivée nX^{n-1} et $nx^{n-1} \neq 0$ (1)
$\forall x \in \{x \in K / x^n = 1\}$

(1) comporte un piège $nx^{n-1} \neq 0$ car $\delta(n,p)=1$, donc $nx^{n-1}=0 \Rightarrow x=0$ et $0 \notin \{x \in K \,/\, x^n = 1\}$.

On a montré que $\# \{x \in K \,/\, x^n = 1\} = n$

Le théorème de Lagrange permet de conclure :

$$n \mid \underbrace{\# K - 1}_{\# K^*}$$

CQFD

b) <u>Soit m' tel que $n \mid q^{m'} - 1$</u>

Posons $q = p^\alpha$ $\qquad q^{m'} = p^{\alpha m'}$

$\exists K'$ de cardinal $\# K' = p^{\alpha m'}$ et tel que $\mathbb{F}_q \hookrightarrow K'$ (car $\alpha \mid \alpha m'$)

$$\begin{array}{ccc} \mathbb{F}_q & \hookrightarrow & K' \\ & \searrow & \nearrow \\ & K & \end{array}$$

<u>Problème</u> : $f = X^n - 1$ se décompose dans K' $\Rightarrow$ K' = corps de décomposition et donc $K' \hookrightarrow K$

$\Downarrow$

$q^{m'} = (q^m)^\beta$ i.e. $m\beta = m'$

$n \mid q^{m'} - 1 \Rightarrow n \mid \# K'^*$ et $(K'^*, \times)$ est cyclique (sous-groupe mult. d'un corps fini) $\Rightarrow \exists!\ G$ sous-groupe de $(K'^*, \times)$

$\Rightarrow G = \{x \in K'^* \,/\, x^n = 1\}$ et $\# G = n$

Donc K' = corps de décomposition de f.

CQFD

c) $p \in \mathcal{P}$: $\begin{cases} \alpha \in \mathbb{N}^* \\ n \in \mathbb{N}^* \end{cases}$ $\quad \Delta(n,p) = 1$

Alors $\exists m \in \mathbb{N}^* \; / \; n \mid p^{\alpha m} - 1$

On utilise le a) et le b)

$q = p^\alpha \quad \mathbb{F}_q \quad f = X^n - 1 \quad \begin{cases} \exists m \\ \mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m} \text{ et } n \mid q^m - 1 \end{cases}$

c.à.d $n \mid p^{\alpha m} - 1$

- Si p n'est pas premier :

$$p = \prod_{\alpha_i > 0} p_i^{\alpha_i}$$

$\exists m_i \quad n \mid p_i^{\alpha_i m_i} - 1$

Prenons $m = \text{ppcm}\, m_i \quad n \mid p_i^{\alpha_i m} - 1$

$$p_i^{\alpha_i m} \equiv 1 \quad [n]$$

$$\Downarrow$$

$$\prod p_i^{\alpha_i m} \equiv 1 \quad [n]$$

CQFD

Remarque : 1) Si $\Delta(n, 10) = 1$, $\exists m$ tel que $n \mid \underbrace{9 \cdots 9}_{m \text{ fois } 9}$ (P)

(Prendre $p = 10$ et $\alpha = 1$)

2) Façons élémentaire de montrer (P)

~~$\frac{a}{b} = x + 10^q y$ et $\exists i \,/\, 10^{i+1} y - z = y$ ou $10^q y \to c_0 \cdots c_1, c_0 c_1 \cdots$~~

(Rappel : Th | $\alpha \in \mathbb{R}$; $\alpha \in \mathbb{Q} \Leftrightarrow$ l'écriture décimale de α est périodique à partir d'un certain rang.)

d'où $(10^{t+1}-1)\alpha = z\beta$ si $y = \frac{\alpha}{\beta}$ $\delta(\alpha,\beta) = 1$

Prenons $\alpha = 1$.

$(n, 10) = 1$

$\frac{1}{n} = \underbrace{N_1 . 10^{-p}}_{\text{partie non périodique}} + 10^{-p} x$ où x est périodique (1)

$x = 0,\underbrace{c_0 \cdots c_i}_{N_2} c_0 \cdots c_i \cdots$

est donc tel que

$10^q x - N_2 = x$ $(q \in \mathbb{N})$

$10^q - N_2 = x \Rightarrow \frac{N_2}{10^q - 1} = x$ (2)

(1) et (2) $\Rightarrow 10^p(10^q - 1) = N n$

$\delta(10^p, n) = 1 \Rightarrow n \mid 10^q - 1$

Exercice (1)

K = corps fini de cardinal q impair

a) Montrer que $1 \neq -1$ b) $\varphi : K^* \to K^*$, $x \mapsto x^2$ est un morphisme de groupes de noyau $\operatorname{Ker}\varphi = \{\pm 1\}$.

En déduire que $H = \{x^2 / x \in K^*\}$ possède $\frac{q-1}{2}$ éléments, et que $\# K^*/H = 2$

c) Critère d'Euler

$x \in K^*$ (q impair) $\quad x^{\frac{q-1}{2}} = \begin{cases} 1 \text{ si } x \in H \\ -1 \text{ sinon.} \end{cases}$ (Ind : th. Fondamental, K^* est cyclique, et $G \subset K^*$ $\#G = d \Leftrightarrow G = \{x \in K^* / x^d = 1\}$)

d) Application : $\exists a \in \mathbb{Z}/p\mathbb{Z}$ $(p \in \mathcal{P})$ $a^2 = -1 \Leftrightarrow p \equiv 1 \ [4]$

Polynômes cyclotomiques :

- Soit $n \geq 1$ $(n \in \mathbb{N})$

Φ_n = polynôme cyclotomique d'indice n si :

$\Phi_n(X) = \prod_{\omega(\xi_i)=n} (X - \xi_i)$ $\quad \omega(\xi) = n \Leftrightarrow \xi$ élément d'ordre n de $\mathbb{C}^*$ ~~où n = 1nf~~ (et ξ racine primitive n-ième de l'unité)

On a : $\boxed{\deg \Phi_n = \varphi(n)}$

On pose $\Phi_1(X) = X - 1$

Calculer $\Phi_{12} = X^4 - X^2 - 1$

Calculer $\Phi_p(X)$ où $p \in \mathcal{P}$. $\boxed{\Phi_p(X) = 1 + \cdots + X^{p-1}}$

Prop 1 | Φ_n est un polynôme à coefficients entiers.

c.à.d $\Phi_n \in \mathbb{Z}[X]$

Prop 2 | On a : $\forall n \in \mathbb{N}$

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Preuve Prop 2 :

$G_d = \{ \xi \in \Gamma_n \ / \ \omega(\xi) = d \}$ où $\Gamma_n = \{ \xi \in \mathbb{C}^* \ / \ \xi^n = 1 \}$

Il est clair que $\Gamma_n = \bigsqcup_{d|n} G_d \Rightarrow X^n - 1 = \prod_{\xi \in \Gamma_n} (X - \xi)$

$$X^n - 1 = \prod_{d|n} \prod_{\xi \in G_d} (X - \xi) = \prod_{d|n} \Phi_d$$

(Note : on retrouve la formule d'Euler $n = \sum_{d|n} \varphi(d)$)

Preuve Prop 1 :

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d}$$

récurrence : (H) Supposons que $\Phi_m \in \mathbb{Z}[X]$ $\forall m < n$.

On est dans la situation suivante $P = \frac{Q}{R}$ $\left.\begin{array}{l} R \text{ monique} \\ Q, R \in \mathbb{Z}[X] \\ P \in \mathbb{C}[X] \end{array}\right\} \Rightarrow P \in \mathbb{Z}[X]$

En effet $PR = Q \Rightarrow$ le coefficient de plus haut degré de P est entier.

coef. $\quad a \ b \quad c$

$\quad P \ R = Q$

deg $\quad p \ r$

$\left\{ \begin{array}{l} a_p \in \mathbb{Z} \\ a_{p-1} \ ? \quad \underbrace{c_{p+r-1}}_{\in \mathbb{Z}} = a_p b_{r-1} + a_{p-1} \underbrace{b_r}_{1} \Rightarrow a_{p-1} \in \mathbb{Z} \text{ cqfd} \end{array} \right.$

② 1°/ $f(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$

Corps des racines de f ?

$$f(X) = X^4 - 6X^2 + 9 + 4X^2$$

$$= (X^2-3)^2 + 4X^2 = (X^2 - 3 - 2iX)(X^2 - 3 + 2iX)$$

$$\Delta' = -1 + 3 = 2$$

d'où les racines $\begin{cases} i \pm \sqrt{2} \\ -i \pm \sqrt{2} \end{cases}$

Le corps des racines de f sur $\mathbb{Q}$ est $\mathbb{Q}(i, \sqrt{2})$

$$[\mathbb{Q}(i,\sqrt{2}) ; \mathbb{Q}] = \underbrace{[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(\sqrt{2})]}_{} \times \underbrace{[\mathbb{Q}(\sqrt{2}) ; \mathbb{Q}]}_{}$$

pol. min. X^2+1 2 pol. min. X^2-2

2°/ $f(X)$ est irréductible sur $\mathbb{Q}$.

On a $f(i+\sqrt{2}) = 0$.

Quel est le degré de $i+\sqrt{2}$ sur $\mathbb{Q}$? (1, 2, 3 ou 4.) (Critère d'Eiseinstein servira pour le partiel)

- $i+\sqrt{2}$ n'est pas de degré 1,
- $i+\sqrt{2}$ était de degré 3, $\exists g \,/\, g(i+\sqrt{2}) = 0$ et $f = gh$

h serait de degré 1 et f admettrait une racine rationnelle, ce qui n'est pas, puis-que ses racines sont $i \pm \sqrt{2}$ $-i \pm \sqrt{2}$.

- Si $i+\sqrt{2}$ était de degré 2, on aurait

$$\exists\, g = X^2 + aX + b \;/\; -1 + 2 + 2i\sqrt{2} + ai + a\sqrt{2} + b = 0$$

$$\Downarrow$$

$$2\sqrt{2} + a = 0 \qquad a \in \mathbb{Q}$$

impossible.

- Donc $i+\sqrt{2}$ est de degré 4, et par suite f est irréductible sur $\mathbb{Q}$

OPFD

Groupe de galois de $f(X) = X^4 - 2X^2 + 9$

On sait que ~~gal(Q(i, √2))~~ $\underbrace{gal_{\mathbb{Q}}(f)}_{}$ $\subseteq S_4$

4 éléments (car f est séparable)

En effet : $gal_{\mathbb{Q}}(f) \hookrightarrow S_{\{x_1,x_2,x_3,x_4\}}$ morphisme injectif

$\theta \longmapsto \theta|_{\{x_1,x_2,x_3,x_4\}}$

Comme f est séparable $\# gal_{\mathbb{Q}}(f) = [\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}] = 4$

Un groupe de cardinal 4 est commutatif (les ordres des éléments ne pouvant être que 1, 2 ou 4)

Donc $gal_{\mathbb{Q}}(f)$ est isomorphe à un groupe $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Soit $\theta \in gal_{\mathbb{Q}}(f)$: $i^2 = -1 \Rightarrow \theta(i) = \pm i$

$(\sqrt{2})^2 = 2 \Rightarrow \theta(\sqrt{2}) = \pm\sqrt{2}$

donc $\begin{cases} \theta^2(i) = i \\ \theta^2(\sqrt{2}) = \sqrt{2} \end{cases}$ (où $\theta^2 = \theta \circ \theta$)

Donc $\theta^2 = Id$.

Tout élément de $gal_{\mathbb{Q}}(f)$ est d'ordre 2. C'est le groupe de Klein.

$$gal_{\mathbb{Q}}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Service de renseignement Klein	SDECE
Indication : tous les exos du Mac-Lane	p 301 (⊃ partie du sujet)

(~ p 299)
298

Important

③ Soit $P \in F[X]$ irréductible

$$\left.\begin{array}{l}\deg P = q \\ \Delta([K:F], q) = 1\end{array}\right\} \Rightarrow P \text{ irréductible sur } K$$

On peut écrire :

$P = fg$ où | f irréductible sur K ~~de~~ et $\deg f = r$
| $f, g \in K[X]$

$$F \longrightarrow K \longrightarrow K[X]/(f) = L \qquad [L:K] = r$$

$F \searrow F[X]/(P) \overset{\ominus}{\nearrow}$

(corps de rupture de P) (corps de rupture de f) (le corps de rupture s'injecte dans tout corps de

$[L:F] = [K:F] \times r$ (1)

$\ominus\!\!\to$ car L possède au moins une racine de P.

(1) $\Rightarrow$ $[L:F] = r[K:F]$

$= q\,[L : F[X]/(P)]$

d'où $r[K:F] = q\,[L : F[X]/(P)]$

$\Downarrow$ (gauss)

$q \mid r$

Mais $r \leq q$, donc $\boxed{q = r}$

Donc $\boxed{P = f \text{ irréductible sur } K.}$

CQFD

Tests

④ Irréductible ou non ?

X^2+3 sur $\mathbb{Q}(\sqrt{7})$ oui

X^2+1 sur $\mathbb{Q}(i\sqrt{2})$ oui car $i = a + bi\sqrt{2}$ $a,b \in \mathbb{Q}$

X^3+8X-2 sur $\mathbb{Q}(\sqrt{2})$

On peut utiliser l'exercice ③ :

⊛ $f \in F[X]$ irréductible
$F \subset K$ de degré premier avec $\deg f$ } $\Rightarrow$ f premier sur K

⊛ Si ce polynôme avait une racine dans ce corps, son corps de rupture s'injecterait dans $\mathbb{Q}(\sqrt{2})$. X^3+8X-2 est irréductible sur $\mathbb{Q}$. Son corps de rupture est de degré 3, et ne peut s'injecter dans $\mathbb{Q}(\sqrt{2})$ de degré 2 sur $\mathbb{Q}$. Donc X^3+8X-2 est irréductible sur $\mathbb{Q}(\sqrt{2})$

⊛ Faire $(a+b\sqrt{2}) = X$ dans X^3+8X-2 et trouver que ce n'est pas possible $(a,b \in \mathbb{Q})$. Comme X^3+8X-2 est de degré 3, X^3+8X-2 irréductible sur $\mathbb{Q} \Leftrightarrow$ pas de racines dans $\mathbb{Q}$.

$f = X^5+3X^3-9X-6$ sur $\mathbb{Q}(\sqrt{7},\sqrt{5},1+i)$

⊛ $[\mathbb{Q}(\sqrt{7},\sqrt{5},1+i) : \mathbb{Q}] = 8 = 2\times 2\times 2$

(car $((1+i)^2-1)^2 = -1 \Rightarrow [\mathbb{Q}(1+i) ; \mathbb{Q}] = 2$)

D'après l'exercice ③, $\deg f = 5$ et $\delta(5,8) = 1 \Rightarrow f$ est irréductible sur $\mathbb{Q}(\sqrt{7},\sqrt{5},1+i)$

$\mathbb{Q} \subset_2 \mathbb{Q}(\sqrt{7}) \subset_2 \mathbb{Q}(\sqrt{7},\sqrt{5}) \subset_2 \mathbb{Q}(\sqrt{7},\sqrt{5},1+i)$

X^2-5 $\qquad$ X^2+1

(Tests) (5) $f \in \mathbb{Q}[X]$ (~~corps K donné~~): Donner $[K : \mathbb{Q}]$

corps des racines de $f = K$

a) $f = X^3 - X^2 - X - 2$

2 est racine évidente $\quad f = (X-2)(\underbrace{X^2 + X + 1}_{j,\, j^2})$

$K = \mathbb{Q}(j)$ de degré 2 sur $\mathbb{Q}$

b) $X^3 - 2 = f \qquad \sqrt[3]{2} \quad j\sqrt[3]{2} \quad j^2\sqrt[3]{2}$

$\mathbb{Q}(j, \sqrt[3]{2})$ de degré 6 sur $\mathbb{Q}$.

car $\quad \underbrace{\mathbb{Q} \subset \mathbb{Q}(j)}_{2} \times \underbrace{\subset \mathbb{Q}(j, \sqrt[3]{2})}_{3}$ (on empile)

c) $X^4 - 7 = f \qquad \begin{cases} \pm\sqrt[4]{7} \\ \pm i\sqrt[4]{7} \end{cases}$

$K = \mathbb{Q}(i, \sqrt[4]{7})$ de degré 8 sur $\mathbb{Q}$

d) $(X^2 - 2)(X^2 - 5)$

$K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ = de degré $2 \times 2 = 4$

Équation du 3^e degré

Soit k un corps de caractéristique $\neq$ de 3 ($\neq$ de 2). Soit $f = X^3 + pX + q$ irréductible de $k[X]$. Soit $k(x_1, x_2, x_3) = K$ le corps des racines de $X^3 + pX + q$.

On a $f(X) = \prod_{i=1}^{3} (X - x_i)$.

Soit $\Delta = \prod_{i<j} (x_i - x_j)$. On pose $D \doteq \mathrm{Discr}(f) = \Delta^2$

On note $G = \mathrm{gal}_k(f) \hookrightarrow \mathcal{S}_{\{x_1, x_2, x_3\}} = \mathcal{S}_3$

Ces racines x_1, x_2, x_3 sont distinctes car f irréductible et k de car. $\neq 3 \Rightarrow f$ séparable.

Soit $\sigma \in G$, $\sigma(\Delta) = \varepsilon_\sigma \Delta \Rightarrow \sigma(D) = D \Rightarrow \underline{D \in k}$

(cf $k = (k(f))^G$)

$H = \{\theta \in G / \theta(\Delta) = \Delta\} = k(\Delta)^G \subset \mathcal{A}_3$ (permutations paires)

Les sous-groupes de $\mathcal{A}_3$ sont : $\mathcal{A}_3$ et $\{Id\}$, donc $H = \mathcal{A}_3$ ou $H = \{Id\}$

Si $H = \{Id\}$, alors $\# G = 2$ ~~$\neq$~~ $= [K ; k] \geq \left[k[X]/(f) ; k \right] = 3$
(car il n'y a pas d'autres sous-groupes d'ordre 3 que ~~...~~ $\mathcal{A}_3 = \{1, (123), (213)\}$) — deg du corps de rupture

Donc $H = \mathcal{A}_3$.

Ainsi $G = \mathcal{S}_3$ ou $\mathcal{A}_3$.

1°/ <u>Si $G = \mathcal{S}_3$</u>, $\exists \theta \in G / \theta(\Delta) = -\Delta \Rightarrow$ $\boxed{\Delta \notin k}$

(si le corps est de caractéristique 2, $-\Delta = \Delta$ et cette implication est fausse.)

2°/ <u>Si $G = \mathcal{A}_3$</u>, $\forall \theta \in G$; $\theta(\Delta) = \Delta \Rightarrow$ $\boxed{\Delta \in k}$

La structure du groupe de Galois est donc parfaitement déterminée par Δ, suivant que $\Delta \in$ ou $\notin$ à k.

Pb : Calculer D

$$f(X) = \prod_i (X - x_i)$$

$$f'(X) = (X-x_1)(X-x_2) + (X-x_2)(X-x_3) + (X-x_3)(X-x_1)$$

$$f'(x_1) f'(x_2) f'(x_3) = -(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 = -D$$

$$-D = (3x_1^2+p)(3x_2^2+p)(3x_3^2+p)$$

Mais $x_i^2 = -p - \frac{q}{x_i} \Rightarrow 3x_i^2 + p = -2p - \frac{3q}{x_i}$

d'où :

- $$D = \left(\frac{3q}{x_1}+2p\right)\left(\frac{3q}{x_2}+2p\right)\left(\frac{3q}{x_3}+2p\right)$$

$$D = \frac{27q^3}{x_1x_2x_3} + \underbrace{18q^2p\left(\frac{1}{x_1x_2}+\frac{1}{x_2x_3}+\frac{1}{x_3x_1}\right)}_{0 \text{ car } x_1+x_2+x_3=0} + 12p^2q\left(\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}\right) + 8p^3$$

$$D = -27q^2 + \frac{12p^3q}{-q} + 8p^3$$

$$D = -27q^2 - 4p^3$$

- $$\boxed{D = -4p^3 - 27q^2}$$

$X^3 + pX + q$

$\begin{cases} D \text{ carré dans } \mathbb{Q} \Leftrightarrow gal_{\mathbb{Q}}(f) = \mathcal{A}_3 \\ D \neq \text{carré dans } \mathbb{Q} \Leftrightarrow gal_{\mathbb{Q}}(f) = \mathcal{S}_3 \end{cases}$

Application :

- $X^3 + 2X + 1 \in \mathbb{Q}[X]$

$D = +32 - 27 = 5$

$\Delta^2 = D \Rightarrow \Delta \notin \mathbb{Q}$ donc $\boxed{G = \mathcal{S}_3}$ ($\Delta = \sqrt{5}$)

- $X^3 - 3X + 1$

$D = 81$ donc $G = \mathcal{A}_3$ cf *

Trisection de l'angle (rien compris)

Tracer les trisectrices d'un angle à la règle et au compas.

On ne peut résoudre à la règle et au compas que les équations de degré 2^n.

$$\cos 3\theta = 4\left(\cos^3\theta - \frac{3}{4}\cos\theta\right) = 4\cos^3\theta - 3\cos\theta$$

Pour $\theta = \frac{\pi}{3}$?, $\cos\frac{\theta}{3}$ est de degré 3 car $4X^3 - 3X + 1 = 0$ est irréductible sur $\mathbb{Q}$

$$X^3 - 3X + 1 = 0$$

(*) $X = u + v$ $\quad X^3 - 3X + 1 = u^3 + v^3 + (u+v)(\underbrace{3uv}_{=1} - 3) + 1 = 0$

$$\begin{cases} u^3 + v^3 = -1 \\ uv = 1 \end{cases}$$

On pose $U = u^3$ $\quad V = v^3$ $\quad \begin{cases} U + V = -1 \\ UV = 1 \end{cases}$ $\quad T^2 + T + 1 = 0$ $\quad \begin{cases} U = j \\ V = j^2 \end{cases}$

$$\begin{cases} U = e^{i\frac{2\pi}{3}} \\ V = e^{-i\frac{2\pi}{3}} \end{cases}$$

Les racines de l'équation $X^3 - 3X + 1$ sont

1) $u = e^{i\frac{2\pi}{9}}$ $\quad v = e^{-i\frac{2\pi}{9}}$; $u + v = 2\cos\frac{2\pi}{9}$

2) $ju + j^2 v = 2\cos\frac{8\pi}{9}$

3) $j^2 u + jv = 2\cos\frac{4\pi}{9}$

On a $\cos 2x = 2\cos^2 x - 1$, donc L = corps de rac. de $X^3 - 3X + 1$

$L = \mathbb{Q}\left(\cos\frac{2\pi}{9}\right)$ $\quad \cos\frac{2\pi}{9}$ de polynôme minimal de $X^3 - 3X + 1 \Rightarrow [L:\mathbb{Q}] = 3 \Rightarrow \text{Gal}(P) = 3 \Rightarrow \text{Gal}_{\mathbb{Q}}(P) = \mathcal{A}_3$ (cf (Δ) page 6)

Propriété universelle du corps de rupture

Th
Def
f polynôme irréductible $k \subset K$ = corps de rupture de f

$\forall k \to L$ tel que $\exists x \in L / f(x) = 0$

Alors $\exists ! \; K \overset{\varphi}{\hookrightarrow} L$ morphisme qui rende le diagramme suivant commutatif :

$$\begin{array}{ccc} & k & \\ \alpha \swarrow & & \searrow \beta \\ K & \xrightarrow[\varphi]{} & L \end{array}$$

$(\beta = \varphi \circ \alpha)$

c'est une définition possible du corps de rupture de f.

Th

$\forall f$ polynôme , $k \subset K$ = corps des racines de f

$\forall k \to L \;/\; f = a \prod (X - x_i) \quad x_i \in L$

$\exists ! \; K \hookrightarrow L$ morphisme qui rende le diagramme

$$\begin{array}{ccc} & k & \\ \swarrow & & \searrow \\ K & \to & L \end{array}$$

Rappel :

A anneau principal (par définition : intègre et tout idéal est monogène)

On a pas de mal à définir la divisibilité :

$a, b \in A \qquad a | b \Leftrightarrow \exists c \in A \;/\; b = ac$

Notons $U = \{x \in A \;/\; \exists y \in A \quad xy = 1\}$. On remarque que $\forall a \in A \; \forall u \in U \quad u | a$ et $ua | a$

$(U, \times)$ = groupe pour la multiplication.

Def : On dit que $a \in A \setminus U$, $a \neq 0$ est irréductible ssi les seuls diviseurs de a sont les diviseurs obligatoires, c.à.d $u \in U$ ou ua.

Def : a et b sont premiers entre eux ssi ils n'ont pas d'autre diviseurs commun que $u \in U$.

Le coté PGCD - PPCM se fait bien.

Si D est un carré dans $\mathbb{Q}$

(Δ) $$(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 = a^2 \qquad a\in\mathbb{Q}.$$

$$\Updownarrow$$

$$(x_1-x_2)(x_1-x_3)(x_2-x_3) = \pm a \qquad (1)$$

$x_3 = -x_1 - x_2$ (voir somme des racines de $\underbrace{X^3+pX+q}_{=P}$)

(1) donne : $(x_1-x_2)(2x_1+x_2)(x_1+2x_2) = a$

$[\mathbb{Q}(x_1):\mathbb{Q}]=3$ car P est irréductible

$(x_1 - X)(2x_1 + X)(x_1+2X) - a \in \mathbb{Q}(x_1)$

et une racine de ce polynôme est x_2

$\ell = [\underbrace{\mathbb{Q}(x_1,x_2)}:\mathbb{Q}(x_1)] \leq 3$

c'est le corps des racines de P

$\ell = 1, 2$ ou 3.

- Si $\ell=3$, le corps des racines de P aurait pour degré $3\times 3 = 9$. Ce n'est pas possible car $\deg[\mathbb{Q}(x_1,x_2):\mathbb{Q}] \leq 3$!

- Si $\ell = 2 \Rightarrow \exists$ diviseur de degré 1.

Corps de rupture d'un polynôme irréductible sur $k[X]$: $P \in k[X]$.

<u>Définition</u> : Soit $P \in k[X]$ un polynôme irréductible sur $k[X]$. On appelle corps de rupture de P tout sur-corps R de k qui vérifie :

1) $\exists x \in R \ / \ P(x) = 0$
2) $\forall K$ corps $k \hookrightarrow K \ / \ \exists x \in K \ P(x) = 0$, alors $R \hookrightarrow K$

On dira que R est un plus petit corps, à isomorphisme près, contenant au moins une racine de $P \in k[X]$.

<u>Pro 1</u> : $k \hookrightarrow k[X]/(P)$ et $\exists \xi \in k[X]/(P) \ / \ P(\xi) = 0$.

<u>Pro 2</u> : $\forall K \ / \ \exists x \in K \ P(x) = 0$ et $k \hookrightarrow K$ alors $k[X]/(P) \hookrightarrow K$

<u>Pro 3</u> : Les corps de rupture sont uniques, à isomorphisme (de corps) près.

Prouvons les 3 propositions :

Pro 1 On considère $\pi : k[X] \longrightarrow k[X]/(P)$, $Q \longmapsto \dot{Q}$ et $\pi|_k = \tilde{\pi}$

$\forall a, b \in k \quad \dot{a} = \dot{b} \Leftrightarrow \dot{\overline{a-b}} = \dot{0} \Leftrightarrow P \mid a-b \Rightarrow a - b = 0$ (cf. P irr.)
$\Rightarrow a = b$.

$\pi|_k = \tilde{\pi}$ est donc injective. C'est un morphisme de corps. Donc $k \hookrightarrow k[X]/(P)$

Montrons l'existence de $\xi \ / \ P(\xi) = 0$:

$\xi = \dot{X} \quad P(\dot{X}) = \dot{\overline{P(X)}} = \dot{0}$ oui

Pro 2

$k \hookrightarrow K$ donc $\exists \ \Phi$ morph. inj. $/ \ k \xrightarrow{\Phi} K$

$$\begin{array}{ccc} k & \xrightarrow{\Phi} & K \\ \downarrow & \nearrow_{\tilde{\Phi}} & \\ k[X]/(P) & & \end{array}$$

où $\begin{cases} \tilde{\Phi}(a) = \Phi(a) & a \in k \\ \tilde{\Phi}(X) = x \in K & \\ (\text{où } x \ / \ P(x) = 0) & \end{cases}$

$\tilde{\Phi}$ ainsi défini ne dépend pas du représentant choisi ?

Si $\dot{f} = \dot{g}$ où $f, g \in k[X]$, on a :

$$\begin{cases} \tilde{\Phi}(f) = \Phi(f)(x) & \left(\text{où } f = \sum_0^n a_i X^i \Rightarrow \Phi(f) = \sum_0^n \Phi(a_i) X^i \in K[X]\right) \\ \tilde{\Phi}(g) = \Phi(g)(x) \end{cases}$$

$\dot{f} = \dot{g} \Leftrightarrow f - g$ divisible par $P \Leftrightarrow f - g = PQ \qquad P, Q \in k[X]$

d'où $\tilde{\Phi}(f) - \tilde{\Phi}(g) = (\Phi(f) - \Phi(g))(x) = \Phi(f-g)(x) = \Phi(PQ)(x)$

$$\tilde{\Phi}(f) - \tilde{\Phi}(g) = \underbrace{\Phi(P)(x)}_{=0 \text{ (car } P(x)=0)} \cdot \Phi(Q)(x) = 0 \quad \text{oui}$$

Pro 3 Unicité des corps de rupture.

R, R' deux corps de rupture de $P \in k[X]$.

Par définition :

$$k \hookrightarrow R', \quad k \hookrightarrow R, \quad R \xrightarrow{\varphi_1} R'$$

car R est de rupture et $\exists x \in R' / P(x) = 0$

$$k \hookrightarrow R, \quad k \hookrightarrow R', \quad R' \xrightarrow{\varphi_2} R$$

(φ_i = morph. inj. de corps)

car R' est de rupture et $\exists x \in R / P(x) = 0$

Prenons $R = k[X]/(P)$ corps de rupture trouvé grâce aux Pro 1 et 2.

$\dim_k R = \deg P < \infty$ donc

$$\begin{cases} k[X]/(P) \xrightarrow{\varphi_1} R' & (1) \quad \varphi_1 \text{ inj} \Rightarrow \dim_k R \leq \dim_k R' \\ R' \xrightarrow{\varphi_2} k[X]/(P) & \varphi_2 \text{ injective} \Rightarrow \dim_k R' \leq \dim_k R < \infty \quad (2) \end{cases}$$

(1) (2) donnent alors : $\dim_k R = \dim_k R' \Rightarrow \varphi_1$ inj est aussi surj $\Rightarrow \varphi_1$ est 1 isomorphisme d'ev.

CQFD

Théorème Important

> $k \hookrightarrow K$ et $P \in k[X]$ irréductible sur k.
> Alors :
> $$\wedge([K:k]\,;\,\deg P) = 1 \Rightarrow P \text{ irréductible sur } K$$

démonstration :

$P \neq$ cte car P irr. sur k

Donc $\exists f$ irréductible sur K / $P = fg$ $\quad f, g \in K[X]$

On a le diagramme :

$$k \hookrightarrow K \hookrightarrow K[X]/(f)$$

$K[X]/(f)$ = corps de rupture de $f \in K[X]$ = possède une racine de P.

$k \hookrightarrow k[X]/(P) \hookrightarrow K[X]/(f)$: prop. universelle des corps de rupture (définition même des corps de rupture !)

$k[X]/(P)$: corps de rupture de $P \in k[X]$

$$\left[K[X]/(f) : k\right] = (\deg f)\,[K:k] = \left[K[X]/(f) : k[X]/(P)\right] \cdot \deg P$$

et (th. gauss) $\deg P \mid \deg f$ or $\deg f \leq \deg P \Rightarrow \deg f = \deg P$

et $P = \text{cte} \cdot f$ où $\text{cte} \in K$, $\text{cte} \neq 0$.

CQFD

…7 page 308

$Gal_F(P)$? où $\begin{cases} F = \mathbb{Q}(\zeta) \text{ et } \zeta = \text{racine 5-primitive de l'unité.} \\ P = X^5 - 7 \end{cases}$

P séparable. Notons L = corps des racines de $P = \mathbb{Q}(r, \zeta) = F(r)$

$\# Gal_F(P) = [L : F] = [F(r) : F]$

Trouvons un polynôme minimal de r sur F.

$X^5 - 7$ est irréductible sur $\mathbb{Q}$.

l'est-il sur $F = \mathbb{Q}(\zeta)$? $[F : \mathbb{Q}] = 4$ et $\deg P = 5$ premiers entre eux.

d'où $[F(r) : F] = 5 \Rightarrow \# gal_F(P) = 5$

Mais $gal_F(P) \subset \mathcal{S}_5$ $\quad \# \mathcal{S}_5 = 5!$ éléments.

Les racines de $P = X^5 - 7$ sont $\{r, \zeta r, \zeta^2 r, \zeta^3 r, \zeta^4 r\}$ toutes distinctes.

Soit $S \in gal_F(P)$ défini par $\begin{cases} S(r) = \zeta r \\ S(\zeta) = \zeta \quad \text{car } \zeta \in F \end{cases}$

On a ~~S(r) = ζr~~

	r	ζr	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$
$S()$	ζr	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$	r

et $S^2(r) = S(\zeta r) = \zeta^2 r$

$S^3(r) = \zeta^3 r$

$S^4(r) = \zeta^4 r$ $\quad \Rightarrow S^5 = Id. \quad \Rightarrow o(S) = 5$

$S^5(r) = r$ $\quad (S^k \neq Id$ si $k < 5)$

S est donc générateur de $gal_F(P) \simeq \mathbb{Z}/5\mathbb{Z}$

Avoir

- F_n irréductible. (voir cours p 4.18)

lemme : P irréductible sur k. Soit K une extension de k :

$\Delta([K : k], \deg P) = 1 \Rightarrow P$ irréductible sur K.

	r	ζr	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$	
$S(\ )$	ζr	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$	r	associé à (12345)
S_2	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$	r	ζr	associé à (13524)
S_3	$\zeta^3 r$	$\zeta^4 r$	r	ζr	$\zeta^2 r$	associé à (14253)
S_4	$\zeta^4 r$	r	ζr	$\zeta^2 r$	$\zeta^3 r$	associé à (15432)
S_5	r	ζr	$\zeta^2 r$	$\zeta^3 r$	$\zeta^4 r$	associé à (1)

<u>Preuve du lemme</u> : Montrer que

$k \hookrightarrow K$

$P \in k[X]$ irréductible sur k.

$\Delta([K:k] ; \deg P) = 1 \Rightarrow P$ irréductible sur K

(oui)

Feuille d'exercice n°1, C_3 Maîtrise

(M. GRANGER)

× ① a) Deux ensembles E et F sont dits <u>équipotents</u>, s'il existe une <u>bijection</u> $f : E \to F$.

Montrer que l'équipolence est une "relation d'équivalence".

On note $\# E$ ou $\operatorname{card} E$ la "classe d'équivalence de E.

b) On note $\operatorname{card} E \leq \operatorname{card} F$, s'il existe une <u>injection</u> $f : E \to F$

Montrer que $\begin{cases} \operatorname{card} E \leq \operatorname{card} F \\ \operatorname{card} F \leq \operatorname{card} E \end{cases} \Rightarrow \operatorname{card} E = \operatorname{card} F$

(théorème de Bernstein.)

<u>Indication</u> : $f : E \to F$ et $g\ F \to E$ étant des injections

construire $\varphi : E \to F$ bijective de façon que :

$$\varphi = f \quad \text{sur } (g \circ f)^n [E - g(F)]$$

$$\varphi = g^{-1} \quad \text{"} (g \circ f)^n \circ g(F - f(E)) \qquad n \in \mathbb{N}$$

c) $\leqslant$ est une relation d'ordre

② a) On appelle groupe cyclique un groupe engendré par un élément. Montrer qu'il est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$

b) Soit $x \in G$, G cyclique d'ordre n, x générateur :

x^k engendre $G \iff k$ et n premiers entre eux.

c) Si G et H sont cyclique d'ordre m, n :

$G \times H$ est cyclique ssi m, n sont premiers entre eux.

d) G fini, $\# G = p$ premier $\Rightarrow G$ est cyclique.

③ Groupe diédral.

Soit $\sigma, r \in \mathfrak{S}_n$ définis par

$$r(i) = i + 1, \text{ si } 1 \leq i \leq n-1 \quad r(n) = 1$$

$$\sigma(i) = n - i + 1, \quad i = 1, \dots, n$$

a) Montrer que $\sigma^2 = 1 \quad r^n = 1$

$$r \circ \sigma \circ r = \sigma$$

b) en déduire que s, r engendre dans σ_n un sous groupe à $2n$ éléments :

$$\Delta_n = \{ Id, r, r^2, \dots, r^{n-1}, \sigma, \sigma \circ r, \dots, \sigma \circ r^{n-1} \}$$

c) Montrer que Δ_n s'identifie aux ~~permutations~~ ~~d'un des~~ isométries d'un polygone régulier à n côtés.

d) Déterminer les sous groupes de Δ_n, les sous groupes distingués.

voir PIR I

(4) On appelle sous groupe dérivé de G, noté DG le sous groupe engendré par les $xyx^{-1}y^{-1}$

a) montrer que $D(G)$ est un sous groupe distingué et que si $H \lhd G$:

$$G/H \text{ commutatif} \iff H \supset DG$$

b) on note $D^2(G) = D(D(G)), \dots, D^n(G) = D(D^{n-1}(G))$

Montrer que les conditions suivantes sont équivalentes

(i) $\exists r \quad D^{r+1}(G) = \{e\}$ e élément neutre de G.

(ii) Il existe des sous groupes H_i $\{e\} = H_0 \subset H_1 \subset \dots \subset H_s = G$ tels que : $H_i \lhd H_{i+1}$ et H_{i+1}/H_i commutatif.

(iii) ~~Mêmes conditions~~ (ii) et en plus $H_i \lhd G$

× (5) ("lemme des cinq")

Soit

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \end{array}$$

un diagramme de groupe commutatif (ie $q \circ f = f' \circ p$ etc...) à lignes exacte

intérêt : " si p, q, s, t sont des isomorphismes de groupes, alors r est un isomorphisme de groupes".

Alors : a) p surjectif, q, s injectifs $\Longrightarrow$ r injectif

b) q, s surjectifs, t injectif $\Longrightarrow$ r surjectif

c) conditions (a)+(b) $\Longrightarrow$ r bijectif

E muni d'une relation d'ordre $\leq$.

Ordre total : $\forall x, y \in E \quad x \leq y$ ou $y \leq x$

Bon ordre : Quel que soit $A \subset E$, $A \neq \emptyset \quad \exists x_0 \in A$ tel que
$x_0 = \text{Inf}\{y \mid y \in A\}$
(c.à.d $x_0 = \text{Min } A$)

1) E bien ordonné $\Rightarrow$ E totalement ordonné. $\mathbb{N}$; $\mathbb{N} \cup \{\infty\}$; $\{0 ; \dots ; n\} = S_n$

2) Donner des exemples d'ensembles bien ordonnés $\mathbb{R}$; $\mathbb{Z}$
" " " totalement ordonnés et non bien ordonnés.

3) $\mathbb{N} \times \mathbb{N} \quad (a, b) \leq (a', b') \Leftrightarrow a < a'$ ou $\{a = a'$ et $b \leq b'\}$
Montrer que l'ordre lexicographique sur $\mathbb{N} \times \mathbb{N}$ est une relation de bon ordre.

4) Tout ensemble bien ordonné admet un plus petit élément.
E bien ordonné $\begin{cases} \text{i)} \forall x \in E \quad \exists y \doteq x+1 \;/\; x < y \text{ et } \forall z > x \quad z \geq y. \\ \text{ou} \qquad \text{(successeur de } x\text{)} \qquad \text{on note } y = x' \\ \text{ii)} \forall y \in E \quad y \leq x \end{cases}$

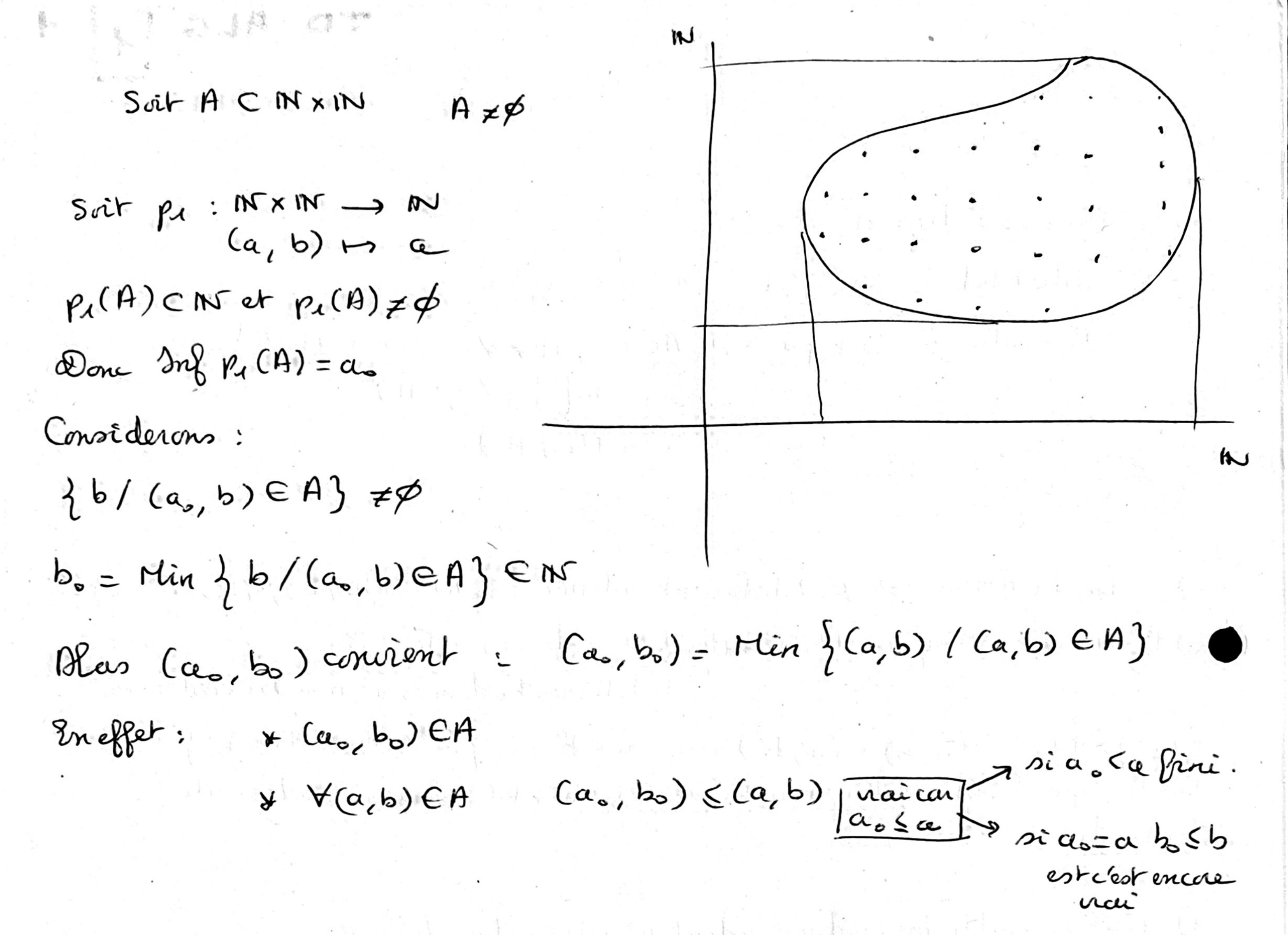
Solutions :

Preuve de 1) $\text{Inf}\{x, y\} = z \in \{x, y\} \Rightarrow z = x$ ou $z = y$

Notations : $S_x = \{y \mid y < x\} \qquad \bar{S}_x = \{y \mid y \leq x\}$

4) $x' = \text{Min}(E \setminus \bar{S}_x)$ ou $E = \bar{S}_x$

3)



Soit $A \subset \mathbb{N} \times \mathbb{N}$ $A \neq \emptyset$

Soit $p_1 : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
$(a, b) \mapsto a$

$p_1(A) \subset \mathbb{N}$ et $p_1(A) \neq \emptyset$

Donc $\text{Inf } p_1(A) = a_0$

Considerons :

$\{ b / (a_0, b) \in A \} \neq \emptyset$

$b_0 = \text{Min} \{ b / (a_0, b) \in A \} \in \mathbb{N}$

Alors (a_0, b_0) convient : $(a_0, b_0) = \text{Min} \{ (a,b) / (a,b) \in A \}$ ●

En effet : $*$ $(a_0, b_0) \in A$

$*$ $\forall (a,b) \in A$ $(a_0, b_0) \leq (a, b)$ | vrai car $a_0 \leq a$ | → si $a_0 < a$ fini. → si $a_0 = a$ $b_0 \leq b$ est c'est encore vrai

Remarque 1 : On aurait pu prendre n'importe quel ensemble E bien ordonné à la place de $\mathbb{N}$.

Remarque 2 : $\forall x \in E$ où E est bien ordonné, S_x est bien ordonné. ●

Ordre inverse : $(E, \leq)$, l'ordre inverse de E est défini par :

$x \prec y \Leftrightarrow y \leq x$

Soit $(E, \leq)$ un bon ordre et $E \neq \emptyset$ $(E, \leq)$ et $(E, \prec)$ sont bien ordonnés $\Leftrightarrow$ E fini

preuve :

$(\Rightarrow)$ Soit $x_0 = \text{Inf } E$ $A = \{ x_0, x_0+1, \ldots, x_0+n, \ldots \} \subset E$

où $x_0 + (n+1) =$ successeur de $x_0 + n$.

Il existe p / $x_0 + p = \text{Sup } A$ donc $A = \{ x_0, \ldots, x_0+p \}$ (1)

Soit $y \in E$. Si $y > x_0 + p$ alors $x_0 + (p+1)$ existerait

car $\{y \in E \,/\, y > x_0 + p\} \neq \emptyset$. Mais alors, $x_0 + p$ ne serait pas le plus grand élément de A, ce qui contredit (1)

• Donc $x_0 \leq y \leq x_0 + p$

Soit $\{k \,/\, x_0 + k \leq y\} \neq \emptyset$. Posons $\underset{k}{\text{Max}} \{k / x_0 + k \leq y\} = k_0$

• 1^er cas $k_0 < p$ $\quad x_0 + k_0 \leq y < x_0 + k_0 + 1$

Et forcément $y = x_0 + k_0$ (sinon, on contredirait le fait que $x_0 + k_0 + 1$ soit le successeur de $x_0 + k_0$)

Ainsi $y \in A$.

• 2^e cas $k_0 = p$ $\quad x_0 + p \leq y \leq x_0 + p \Rightarrow y = x_0 + p \in A$

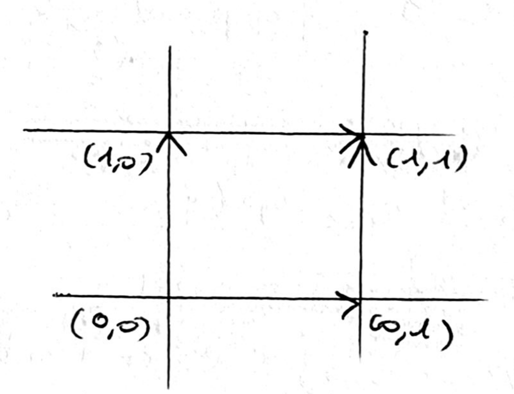
D'où $E = A$ est fini.

($\Leftarrow$) Évident, puisque $(E, \leq)$ est bien ordonné et E fini.

2

$A \times B$ $\quad$ A, B ordonnés

L'<u>ordre produit</u> sur $A \times B$: $\quad (a,b) \leq (a',b') \Leftrightarrow \begin{cases} a \leq a' \\ \text{et} \\ b \leq b' \end{cases}$



les éléments (1,0) et (0,1) ne sont pas comparables.

$\{0,1\} \times \{0,1\}$ <u>n'est pas totalement ordonné</u>.

<u>Remarque</u> : Deuxième démonstration

Posons $V = \{x \,/\, S_x \text{ est fini}\}$ et $y_0 = \text{Max } V$. Montrer que $E = S_{y_0} \cup \{y_0\}$

Th (lemme) | E ensemble, $\mathfrak{S} \subset \mathcal{P}(E)$ ($\mathfrak{S}$ = S gothique)

$\mathfrak{S} \xrightarrow{p} E \quad p(X) \notin X$

Alors il existe $M \notin \mathfrak{S}$ muni d'un bon ordre tel que

$\forall x \in M \quad \begin{cases} S_x \in \mathfrak{S} \\ p(S_x) = x \end{cases}$ où $S_x = (\leftarrow, x[$

Remarque : 1) $E \notin \mathfrak{S}$

2) Si $\emptyset \notin \mathfrak{S}$, alors $M = \emptyset$ convient.

Si M convient et $M \neq \emptyset$, $x_0 = \text{Min}\, M$ et $S_{x_0} = \emptyset \in \mathfrak{S}$ impossible.

Donc si $\emptyset \notin \mathfrak{S}$, $M = \emptyset$ convient et c'est le seul qui convienne !

| cas I : E est fini |

On suppose désormais que $\emptyset \in \mathfrak{S}$.

(Si M existe, soit $x_0 = \text{Min}\, M \Rightarrow x_0) = p(S_{x_0}) = p(\emptyset)$)

Posons donc $x_0 = p(\emptyset)$.

Si $\{x_0\} \notin \mathfrak{S}$, on prend $M = \{x_0\}$

Sinon $\{x_0\} \in \mathfrak{S}$, on prend $x_1 = p(\{x_0\})$

Supposons définis par récurrence $x_0, \dots, x_n$ tels que $\{x_0, \dots, x_i\} \in \mathfrak{S}$

pour $i \leq n-1$ et $x_{i+1} = p(\{x_0, \dots, x_i\})$

2 cas : * $\{x_0, \dots, x_n\}$ convient

ou * $\{x_0, \dots, x_n\} \in \mathfrak{S}$ et l'on définit $x_{n+1} = p(\{x_0, \dots, x_n\})$

Si E est fini, l'opération s'arrête nécessairement.

Remarque : Si l'opération ne s'arrête pas, :

$A = \{x_0, \dots, x_n, \dots\}$ — suite bien ordonnée (infinie)

si $A \notin \mathfrak{S}$ c'est fini

sinon $p(\{x_0, \dots, x_n, \dots\}) = x'_0$

d'où
$\{x_0, x_1, \dots, x_n, \dots\}$
$\{x'_0, \dots\}$
$\dots$

Cas général E ensemble $\mathfrak{S} \subset \mathcal{P}(E)$

$p : \mathfrak{S} \to E \quad p(X) \notin X$

$\exists M$ bien ordonné 1) $M \notin \mathfrak{S}$

2) $\forall x \in M \quad \begin{cases} S_x \in \mathfrak{S} \text{ où } S_x =]\leftarrow, x[. \\ p(S_x) = x \end{cases}$

* $E \notin \mathfrak{S}$
* Si $\emptyset \notin \mathfrak{S}$ alors $M = \emptyset$ convient.
* $\emptyset \in \mathfrak{S}$

Soit $\mathcal{M} \subset \mathcal{P}(E)$ défini par $U \in \mathcal{M} \Leftrightarrow U$ bien ordonné et $\forall x \in U \quad S_{U,x} \in \mathfrak{S}$ et $p(S_{U,x}) = x$

Alors $M = \bigcup_{U \in \mathcal{M}} U$ répondra à la question.

$U, U' \in \mathcal{M}$, soit $V \subset U \cap U'$

- premier élément de U ou de U' : $x_0 = p(\emptyset)$
- $V = \{x \in U \cap U' \ / \ S_{U,x} = S_{U',x}$ et l'ordre induit par U et U' est le m̂$\}$
- Si $U \setminus V \neq \emptyset$ et si $U' \setminus V \neq \emptyset$ on pose $\begin{cases} x = \text{Min}_U (U \setminus V) \Rightarrow S_{U,x} = V \\ x' = \text{Min}_{U'} (U' \setminus V) \Rightarrow S_{U',x'} = V \end{cases}$

Donc $V \in \mathfrak{S}$ et $p(V) = x = x' \Rightarrow \underset{x'}{\overset{x}{\shortparallel}} \in V$ impossible

Donc $U \setminus V = \emptyset$ ou $U' \setminus V = \emptyset \Leftrightarrow V = U$ ou $V = U' \Leftrightarrow$ **$U \subset U'$ ou $U' \subset U$**

On pose alors $M = \bigcup_{U \in \mathcal{M}} U$

$\begin{cases} x \in M \\ y \in M \end{cases} \Rightarrow \exists U \in \mathcal{M} \ / \ \begin{matrix} x \in U \\ y \in U \end{matrix}$

$x \leq y$ dans $M \Leftrightarrow x \leq y$ dans U * <u>ne dépend pas de U car</u>

$\left| \begin{array}{l} x \in U \subset U' \\ y \in U \subset U' \end{array} \right. \Rightarrow$ l'ordre $x \leq y$ dans $U \Leftrightarrow x \leq y$ dans U'

* M est bien ordonné.

(NB : Si $x \in U$ et si $y \in M$ / $y \leq_U x$ alors $y \in U$)

~~Remarquer que $x \in U$~~ ~~$y \underset{M}{\leq} x$ alors $y \in U$~~

$\emptyset \neq A \subset M$ $\quad x \in A$ $\quad \exists U \in \mathcal{M}$ / $x \in U$ alors $A \cap U \neq \emptyset$

~~$y \leq x \Rightarrow y \in U$~~

U est bien ordonné et $A \cap U \neq \emptyset \Rightarrow \exists x_0 = \underset{U}{\text{Min}}(A \cap U)$

Alors $x_0 = \underset{M}{\text{Min}}\, A$: $y \in A$ et $y \leq x_0 \Rightarrow y \in U \Rightarrow y \in A \cap U$

$\Rightarrow y = x_0$ et $x_0 \in A$

donc x_0 = élément minimal de A dans A (bien ordonné) ~~et $x_0 \in A$~~

$\Downarrow$

$x_0 = \text{Min}\, A$

* $S_{M,x} = S_{U,x}$ (si $x \in U$)

* $M \notin \mathcal{G}$ $\quad$ Si $M \in \mathcal{G}$ $\quad p(M) = a \notin M$ et $M \cup \{a\} \in \mathcal{M}$

~~Mais alors~~ (car $M \cup \{a\}$ est aussi un ensemble bien ordonné, ~~donc~~ et $p(M) = p(S_a)) = a \notin M$

ce qui est absurde puisque $M = \bigcup_{U \in \mathcal{M}} U$

Théorème de Zermelo.

Tout ensemble E peut être bien ordonné.

preuve :

$\mathcal{G} = \mathcal{P}(E) \setminus \{E\}$

$p : \mathcal{G} \longrightarrow E$

$X \longmapsto \tau_X \in E \setminus X$ $\quad$ car $E \setminus X \neq \emptyset$ $\quad$ (C)

[(Axiome du choix)

$(X_i)_{i \in I}$ famille d'ensemble indexée par I.

$$\forall i \in I \quad X_i \neq \emptyset \iff \prod_{i \in I} X_i \neq \emptyset$$

] La ligne (C) montre le choix d'un élément du produit $\prod_{X \in \mathfrak{S}} (E \setminus X)$

D'après le lemme (si dur à montrer)
$\exists M \subset E$ bien ordonné tel que $M \notin \mathfrak{S} \Rightarrow M = E$ bien ordonné.

•

Remarque : L'axiome du choix est équivalent au théorème de Zorn.

Théorème de Zorn

Tout ensemble ordonné inductif admet un élément maximal

• $(E, \leq)$ est dit inductif si $F \subset E$ F totalement ordonné $\Rightarrow$ F possède un majorant.

On montre le théorème suivant, plus fort que le théorème de Zorn :

Th { Tout ensemble dans lequel les parties bien ordonnées sont majoré admet un élément maximal.

$\mathfrak{S} \subset \mathcal{P}(E)$ tel que $\mathfrak{S} = \{ A \in \mathcal{P}(E) \,/\, A$ bien ordonné et il existe m_A majorant strict de A$\}$

$p : \mathfrak{S} \longrightarrow E$
$A \longmapsto p(A)$ majorant strict de A

$\exists M$ bien ordonné / $\forall x \in M \quad S_x \in M$ et $p(S_x) = x$
et $M \notin \mathfrak{S}$

(*) Si l'ordre sur M ~~et~~ est l'ordre induit par l'ordre sur E. Alors M est une partie bien ordonnée de E, donc M admet un majorant. et $M \notin \mathcal{G} \Rightarrow m \in M$.

Donc m = élément maximal de M

(*) [Montrons (*) que : $y \underset{M}{\leq} x \Rightarrow y \underset{E}{\leq} x$

$$\Downarrow$$

$y \in S_x \quad x = p(S_x) =$ majorant au sens de E

$$\Downarrow$$

$$y \underset{E}{\leq} x$$

Inversement, si $y \underset{E}{\not\leq} x$, on a $y \underset{M}{<} x$ ou $x \underset{M}{<} y$, le cas où $x \underset{M}{<} y$ est exclus par le sens direct. Donc $y \underset{M}{\leq} x$.

Ainsi $y \underset{M}{\leq} x \Leftrightarrow y \underset{E}{\leq} x$

] CQFD

Base d'un espace vectoriel

Soit E un e.v. $\{x_i\}_{i \in I} \subset E$

<u>Définition</u> : Une famille d'éléments de E est linéairement indépendante (ou "libre") si

$$\forall J \subset I \text{ fini} \quad \sum_{i \in J} \lambda_i x_i = 0 \Rightarrow \forall i \in J \ \lambda_i = 0$$

↑

<u>Définition</u> : Une famille $\{x_i\}_{i \in I} = \mathcal{F}$ de E est une base si c'est

1) une famille libre

2) génératrice de E (c.à.d $\forall x \in E \ \exists J$ fini $\exists \lambda_i \ / \ x = \sum_{i \in J} \lambda_i x_i$)

(C'est la définition algébrique des base)

Alors, avec ces définitions :

① Les familles libres forment un système inductif pour $\subset$

② libre + maximale $\Rightarrow$ génératrice.

① $\mathcal{F}'$ = ensemble de familles libres F telle que

$$\forall F, F' \in \mathcal{F}' \qquad F \subset F' \text{ ou } F' \subset F$$

Soit $G = \bigcup_{F \in \mathcal{F}'} F$. Montrons que G est une famille libre :

$$\forall \{x_1, \dots, x_n\} \subset G \text{ fini} \quad \sum_{i=1}^{n} \lambda_i x_i = 0$$

$\forall i \ \exists F_i \quad x_i \in F_i$

On peut supposer que $F_1 \subset \dots \subset F_n$, d'où $x_i \in F_n \quad \forall i \in [1,n]$

Mais $\sum_{i=1}^{n} \lambda_i x_i = 0$ est une relation ne faisant intervenir que des vecteurs de F_n, donc $\lambda_i = 0 \quad \forall i$

Donc G est une famille libre. D'évidence $G \supset F \quad \forall F \in \mathcal{F}'$

Soit B une partie libre maximale.

② Soit $x \in E$. $\quad$ * Si $x \in B \quad x = 1.x$

* $x \notin B \quad B \cup \{x\}$ non libre.

Donc $\exists x_1, \dots, x_n \in B \quad \exists \lambda_i \qquad \lambda_1 x_1 + \dots + \lambda_n x_n + \lambda x = 0$

avec $(\lambda_1, \dots, \lambda) = (0, \dots, 0)$. Alors $\lambda \neq 0$ et $x = \frac{\lambda_1}{\lambda} x_1 + \dots + \frac{\lambda_n}{\lambda}$

et $x \in \langle B \rangle$ (ev engendré par les B)

Donc B est une base.

Exercices :

① A anneau commutatif unitaire. Montrer, en utilisant le théorème de Zorn, que l'ensemble des idéaux propres de A est inductif.
Montrer que pour tout idéal $I \subsetneq A$, il existe M maximal tel que $I \subset M \subsetneq A$.

② Posons $\mathbb{N}^{(\mathbb{N})} = \{ (n_1, n_2, \dots, n_p, \dots) \;/\; n_i \in \mathbb{N} ; \exists p_0 \;\; n_p = 0 \text{ pour } p \geq p_0 \}$

$\mathbb{N}^{(\mathbb{N})}$ est dénombrable. Je le munis de l'ordre lexicographique $\leq$.
~~Montrer qu'~~il est bien ordonné pour $\leq$.
Cependant, l'ordre lexicographique n'est pas un bon ordre sur $\mathbb{N}^{\mathbb{N}}$.

Solutions :

① $(A, +, \times, e)$

Soit $\mathcal{I}$ l'ensemble des idéaux propres de A.

1°) $\mathcal{I}$ est inductif : Soit $\mathcal{F}$ une famille totalement ordonnée pour l'$\subset$.

Alors $\bigcup_{I \in \mathcal{F}} I \in \mathcal{I}$ est un majorant de $\mathcal{F}$, dans $\mathcal{I}$.

Montrons que $\bigcup_{I \in \mathcal{F}} I \in \mathcal{I}$: $\bigcup_{I \in \mathcal{F}} I$ est bien un sous-groupe additif de $(A, +)$ en vertu de l'hypothèse "totalement ordonnée" pour $\mathcal{F}$. Le fait que $\bigcup_{I \in \mathcal{F}} I$ soit un idéal est alors évident :

$$\forall x \in A \quad \forall y \in \bigcup_{I \in \mathcal{F}} I \quad \exists I \in \mathcal{F} \,/\, y \in I \text{ et alors } xy \in I \subset \bigcup_{I \in \mathcal{F}} I$$

Le théorème de Zorn s'applique donc à $\mathcal{I}$: $\mathcal{I}$ possède un élément maximal. Enonçons le résultat :

" Tout anneau commutatif unitaire possède au moins un idéal maximal ".

2°/ Soit I un idéal de A. Soit $\mathcal{J}_I = \{ J$ idéal de A / $J \neq A$ et $J \supset I \}$

$\mathcal{J}_I$ est non vide car $I \in \mathcal{J}_I$. On montre, de la même manière qu'au 1°/, que $\mathcal{J}_I$ est un ensemble inductif pour l'$\subset$. Le théorème de Zorn nous indique qu'il existe $M \in \mathcal{J}_I$ maximal.

M est donc un idéal, maximal dans $\mathcal{J}_I$.

$\forall F$ idéal propre de I tel que $F \supset M$ alors $F \supset I \Rightarrow F \in \mathcal{J}_I$ et $F \supset M \Rightarrow F = M$, ce qui montre que M est aussi un idéal maximal dans l'ensemble $\mathcal{J}$ des idéaux propres de A.

Énonçons le résultat :

" Soit I un idéal de A. Il existe un idéal maximal M tel que $I \subset M$. "

(2) $\mathbb{N}^{(\mathbb{N})}$ est dénombrable comme réunion dénombrable d'ensembles dénombrables.

Ni $\mathbb{N}^{(\mathbb{N})}$, ni $\mathbb{N}^{\mathbb{N}}$ ne sont bien ordonnés pour l'ordre lexicographique.

En effet : soit $A = \{ x_p = (0,0,\dots,0,1,0\dots) \ / \ p \in \mathbb{N}^* \} \subset \mathbb{N}^{(\mathbb{N})} \subset \mathbb{N}^{\mathbb{N}}$

Lemme : Si $n \leq x_p$ alors $n_1 = \dots = n_{p-1} = 0 \quad (p \geqslant 2)$

(où $n = (n_1, \dots))$

Le seul minorant de A possible est $0 = (0, \dots)$

Si $\mathbb{N}^{(\mathbb{N})}$ était bien ordonné, la partie non vide $A \subset \mathbb{N}^{(\mathbb{N})}$ admettrait un minimum, et ce ne peut être que 0. Mais $0 \notin A$. Donc $\mathbb{N}^{(\mathbb{N})}$ n'est pas bien ordonné.

Construisons un bon ordre sur $\mathbb{N}^{(\mathbb{N})}$: Pour tout p, on a une injection

$$\varphi_p : \mathbb{N}^p \longrightarrow \mathbb{N}^{(\mathbb{N})}$$

$$(a_1, \dots, a_p) \longmapsto (a_1, \dots, a_p, 0 \dots)$$

On a $\quad \varphi_p(\mathbb{N}^p) \subset \varphi_{p+1}(\mathbb{N}^{p+1})$

$\quad\quad \| $

$\varphi_{p+1}(\mathbb{N}^p \times \{0\})$

et : $\quad \mathbb{N}^{(\mathbb{N})} = \bigcup_{p \in \mathbb{N}^*} \mathbb{N}^p$

$$\begin{cases} a = (a_1, \dots, a_p, \dots) \\ b = (b_1, \dots, b_p, \dots) \end{cases} \quad a \neq b$$

Je dis que : $\quad a < b \iff \left\{ \exists p \in \mathbb{N}^* / \begin{cases} 1)\ a_i = b_i \quad i > p \\ 2)\ a_p < b_p \end{cases} \right\}$

En d'autres termes, $a_p < b_p$ où $p = \operatorname{Sup}\{k / a_k \neq b_k\}$. Ce Sup existe car $\{k / a_k \neq b_k\}$ est forcément fini.

1°/ $(\mathbb{N}^{(\mathbb{N})}, \leqslant)$ induit sur $\varphi_p(\mathbb{N}^p)$ l'ordre "anti-lexicographique"

2°/ Si $\left.\begin{array}{l} (\underline{a}) \notin \varphi_p(\mathbb{N}^p) \\ (\underline{b}) \in \varphi_p(\mathbb{N}^p) \end{array}\right\} \Rightarrow (\underline{b}) < (\underline{a})$

3°/ $\exists p \quad A \cap \varphi_p(\mathbb{N}^p) \neq \emptyset \quad\quad \operatorname{Min}(A \cap \varphi_p(\mathbb{N}^p))$

4°/ successeur de $\varphi_p(\mathbb{N}^p)$: e_{p+1}

Remarque :

lemme : (E_n) dénombrable $\Rightarrow \bigcup_{n \in \mathbb{N}} E_n$ est dénombrable.

preuve 1 :

$a_{n,p}$ p^- élément de E_n

$F_k = \{ a_{n,p} \; / \; n+p = k \}$ est fini (possède $k+1$ éléments)

D'où $E = \bigcup_{k \in \mathbb{N}} F_k$

preuve 2 : $(a_1, \dots, a_p) \longrightarrow (a_1, \dots, a_p, 0, \dots) = (\underline{a})$

$F'_k = \{ (\underline{a}) \quad a_1 + \dots + a_p \leq k \}$
$p \leq k$

- F'_k est fini et $\mathbb{N}^{(\mathbb{N})} = \bigcup_{k \in \mathbb{N}} F'_k$
- (F'_k) sont emboîtés : $F'_k \subset F'_{k+1}$

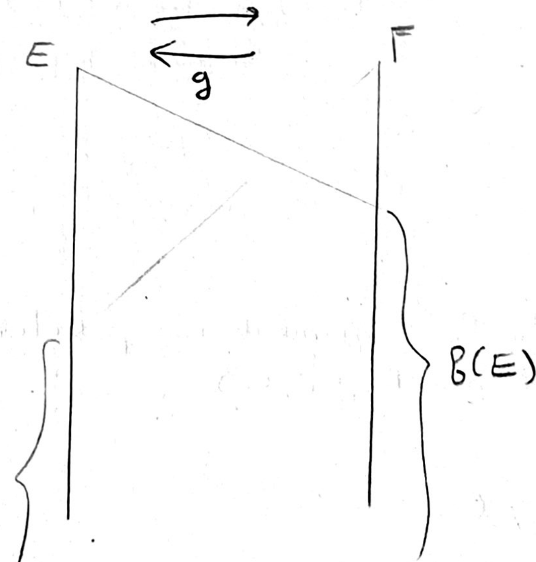
TD ALG [1] (feuille TD)

1) a)

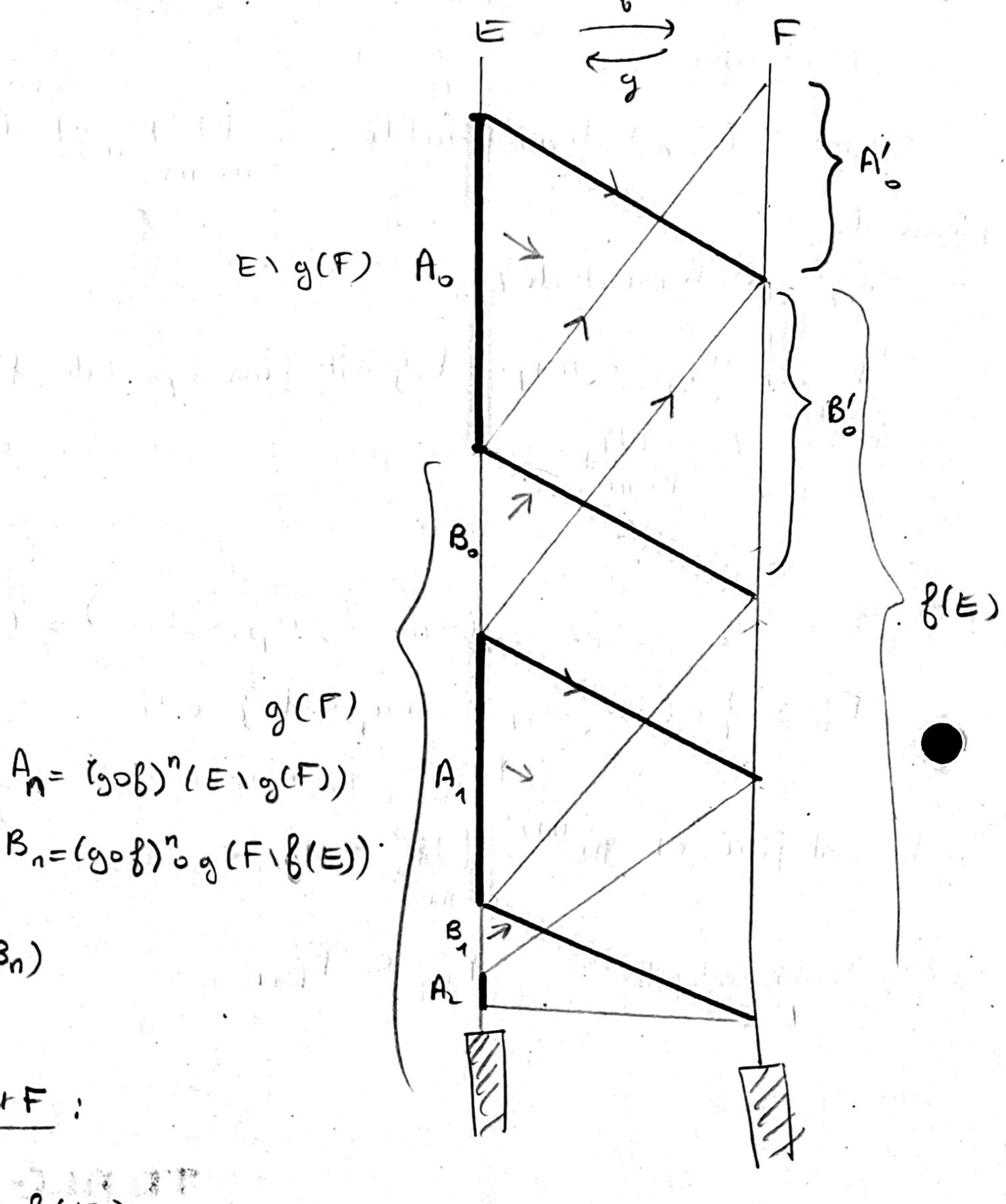
b) * $Id : E \to E$ est injective, donc $\text{Card} E \leq \text{Card} E$

* Théorème de Bernstein : (1890)

$\begin{cases} f : E \to F \\ g : F \to E \end{cases}$ injections



R
A
T



$A_n = (g \circ f)^n (E \setminus g(F))$

$B_n = (g \circ f)^n \circ g(F \setminus f(E))$

Soit $C = E \setminus \bigcup_{n \in \mathbb{N}} (A_n \cup B_n)$

on intervertit f et g, E et F :

$A'_n = (f \circ g)^n (F \setminus f(E))$

$B'_n = (f \circ g)^n \circ f(E \setminus g(F))$

$C' = F \setminus \bigcup_{n \in \mathbb{N}} (A'_n \cup B'_n)$

Alors :

$\varphi(A_n) = f \circ (g \circ f)^n (E \setminus g(F)) = (f \circ g)^n \circ f(E \setminus g(F)) = B'_n$

(c'est vrai grâce à l'associativité de o $f \circ (g \circ f) \circ \dots \circ (g \circ f)$)

$\varphi(B_n) = g^{-1}(B_n) = A'_n$

1) Les A_n, B_n, C forment une partition de E c.à.d $A_n \cap B_m = \emptyset$
(de même pour A'_n, B'_n, C)

si $n \neq m$ $\begin{cases} A_n \cap A_m = \emptyset \\ B_n \cap B_m = \emptyset \end{cases}$

2) $f(C) = C'$

* $f(C) \subset C'$ si $f(x) = y$ $x \in C$, si $y \notin C'$ on aurai $y \in B'_n = f(A_n) \Rightarrow y = f(x')$ $x' \in A_n$ absurde

• ~~*~~ ou bien $y \in A'_n$ $\quad n \geq 1$ (sinon $y \in (F \setminus f(E))$)

et $y \in (f \circ g) \circ \dots \circ (f \circ g)(F \setminus f(E)) = f(B'_{n-1})$.

* <u>$f(C) \supset C'$</u>

~~$C' \subset f(C) \Rightarrow C' \in f(E) \equiv F \cap A'_0$.~~

~~Soit $y \in C'$. $y = f(x)$~~

$C' \subset f(E)$ donc $\exists x \in E$ / $\quad y = f(x)$ $\quad$ où $y \in C'$

Si $x \in A_n$, on aurait $y \in B'_n$
Si $x \in B_n$, on aurait $y \in A'_{n+1}$ ~~donc~~

Donc $x \in C$.

Ainsi $f(C) = C'$, et f injective $\Rightarrow$ f bijective de C sur C'.

<u>Résultat</u> : φ est bijective de E sur F

(<u>Remarque</u> : l'ordre $\leq$ ainsi défini dans la classe des ensembles est une relation de bon ordre. Il existe donc un successeur à $\mathbb{N}$ pour cette relation.)

⑤ "lemme des cinq" : tous des groupes, tous des homomorphismes.

$$\begin{array}{ccccccccc} & & 0 & & & & 0 & & \\ & & \downarrow & & & & \downarrow & & \\ A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \\ \downarrow & & & & & & & & \\ 0 & & & & & & & & \end{array}$$

C'est un diagramme commutatif,

$$\begin{cases} q \circ f = f' \circ p \\ r \circ g = g' \circ q \end{cases}$$

$r \circ g \circ f = g' \circ q \circ f = g' \circ f' \circ p$

etc
...

à lignes exactes : ce qui signifie que toutes les lignes sont des suites exactes.

$0 \longrightarrow A \xrightarrow{f} B$ exacte $\Leftrightarrow$ v injective

$A \xrightarrow{f} B \longrightarrow 0$ exacte $\Leftrightarrow$ f surjective

a) p surjectif, q et s injectives.

$x \in C$ $\quad r(x) = 0 \overset{?}{\Rightarrow} x = 0$

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \\ \downarrow & & & & & & & & \\ 0 & & & & & & & & \end{array}$$

$a \in A$, $b \mapsto x$, $a' \in A'$

Soit x tel que $x \in C$ et $r(x) = 0$

$$h' \circ r(x) = s \circ h(x) = 0 \underset{(s\ inj)}{\Rightarrow} h(x) = 0 \Leftrightarrow x \in \ker h \Rightarrow \exists b \in B \,/\, g(b) = x$$

Or $\quad g' \circ q(b) = r \circ \underbrace{g(b)}_{x} \Rightarrow q(b) \in \ker g' = \operatorname{Im} f' \Rightarrow \exists a' \,/\, f'(a') = q(b)$

$\exists a \in A \,/\, a' = p(a)$

$q(b) = f' \circ p(a)$

$\Rightarrow f' \circ p(a) = q \circ f(a) \underset{(q\ injective)}{\Rightarrow} f(a) = b \Rightarrow g(b) = 0$

Mais $g(b) = x$! donc $x = 0$.

CQFD

b) q et s surjectives, t injectif ⇒ r surjectif

$$\begin{array}{ccccccccc} & & & & & & & & 0 \\ & & & & & & & & \downarrow \\ A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \\ & & \downarrow & & & & \downarrow & & \\ & & 0 & & & & 0 & & \end{array}$$

$x' \in C'$ Posons : $\exists x \in C \,/\, r(x) = x'$

Soit $y' = h'(x')$ s est surjective : $\exists y \in D \,/\, s(y) = y'$

Alors $k' \circ s(y) = 0 = t \circ k(y)$

$\Downarrow$ (t injective)

$k(y) = 0$

donc $y \in \operatorname{Ker} k = \operatorname{Im} h$

$\exists x_1 \in C \,/\, h(x_1) = y$

Notons $r(x_1) = x_1'$

Mais $h'(x_1') = h'(x_2')$ puisque $\begin{cases} h'(x_2') = y' \\ \text{et} \\ s \circ h(x_1) = h' \circ r(x_1) \end{cases}$

$\underbrace{s \circ \underbrace{h(x_1)}_{y}}_{y'}$, $\underbrace{r(x_1)}_{x_1'}$

~~D'où $h'(x_1' x_2'^{-1}) = 0$~~

Posons $\xi' = x_1' x'^{-1}$ alors $h'(\xi') = 0$

Donc $\xi' \in \operatorname{Ker} h' = \operatorname{Im} g'$ $\Rightarrow \exists z' \in B'$ $g'(z') = \xi'$

$\exists z \in B \,/\, q(z) = z'$ puisque q est surjective

D'où $\xi' = g' \circ q(z) = r \circ g(z)$

Ainsi $x_1' x'^{-1} = r \circ g(z)$

$\Downarrow$

$r(x_1) x'^{-1} = r(g(z))$

$\Downarrow$

$$\boxed{x' = r[x_1 \, g(z)^{-1}]}$$

r est bien surjective.

c) r bijectif dès que $\begin{cases} q, s \text{ bijectives} \\ p \text{ surjectif et } t \text{ injectif} \end{cases}$

$$\begin{array}{ccccccccc} & & 0 & & & & 0 & & 0 \\ & & \downarrow & & & & \downarrow & & \downarrow \\ A & \to & B & \to & C & \to & D & \to & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \to & B' & \to & C' & \to & D' & \to & E' \\ \downarrow & & \downarrow & & & & \downarrow & & \\ 0 & & 0 & & & & 0 & & \end{array}$$

(2) H_A = sous-groupe engendré par $A = \bigcap \{ H \,/\, H$ sous-groupe de $G \,/\, H \supset A \}$

Alors $H_A = \{ a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k} \,,\, \varepsilon_i = \pm 1$ et $a_i \in A \cup \{e\} \}$

(▫ H_A est un sous-groupe, et si S sous-groupe $S \supset A$ alors $S \supset H_A$.
($H_A \supset A$) donc H_A = minimum des S contenant A.)

$H_a = \{ a^n \,/\, n \in \mathbb{Z} \}$ est commutatif.

a) b) facile.

c) $\delta(m,n) = 1 \overset{(1)}{\Longrightarrow}$ $G \times H$ cyclique (facile)

$G \times H$ cyclique $\Longrightarrow \Delta(m,n) = 1$

- Supposons que $G \times H$ soit engendré par (x,y). Alors x engendre G et

(TB) y engendre H. ~~D'après l'aller~~ D'après l'aller (1), (x,y) engendre un groupe à $c = \mu(\underbrace{\omega(x)}_{m}, \underbrace{\omega(y)}_{n})$ éléments.

Donc $\mu(m,n) = mn \Longleftrightarrow \delta(m,n) = 1$

Remarque :

Tout revient à montrer ~~que~~ le lemme suivant :

$$\boxed{\omega((x,y)) = \text{ppcm}\,(\omega(x), \omega(y))}$$

- Application

$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \simeq \overbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}}$

Dans G $\quad \omega((1,1)) = \text{ppcm}(\omega(1), \omega(1)) = \text{ppcm}(6,14) = 42$

donc $\langle (1,1) \rangle \neq G$.

d) classique.

Remarque :

$G \times H$ cyclique $\Leftrightarrow$ G cyclique, H cyclique et $\Delta(\#G, \#H) = 1$

$\Downarrow$

Théorème Chinois

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

dès que $\Delta(a,b) = 1$

$\longrightarrow$ Se rappeler de la résolution du système de congruence :

$$\begin{cases} k \equiv i & [n] \\ k \equiv j & [m] \end{cases}$$

qui admet des solutions si $\Delta(m,n) = 1$.
La solution est alors unique modulo $\mu(m,n)$

③ a)

b) $\sigma^2 = 1$
$r^n = 1$
$r\sigma r = \sigma \Rightarrow r\sigma = \sigma r^{-1}$

$H_{\sigma r} = \{ \sigma^{n_1} r^{m_1} \dots \sigma^{n_p} r^{m_p} \ / \ n_i, m_i \in \mathbb{Z} \}$

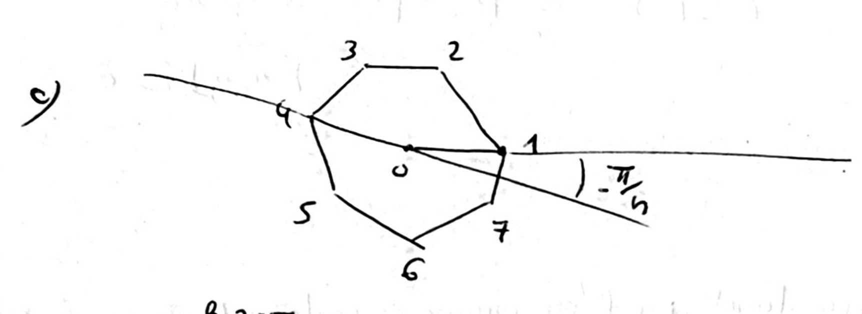
On peut prendre $\begin{cases} n_i = 0 \text{ ou } 1 \\ m_i = 0, \dots, n-1 \end{cases}$

Alors $\Delta_n = \{ Id, r, r^2, \dots, r^{n-1}, \sigma, \sigma r, \dots, \sigma r^{n-1} \}$ est le sgroupe engendré par r et σ.

En effet :
1) Δ_n est un groupe et $\Delta_n = \langle r \rangle \cup \sigma \langle r \rangle$
2) Δ_n contient r et σ
3) $\forall G$ groupe / G contient r et σ, $\Rightarrow G \supset \Delta_n$

Ce groupe Δ_n possède $2n$ éléments :

c)



- $H_n = \left\{ e^{\frac{k2i\pi}{n}}, k \in [1,n] \right\} \xrightarrow{\sim} \Delta_n = \{1, \dots, r^{n-1}, \sigma, \dots, \sigma r^{n-1}\}$

où $\begin{cases} r = \text{rotation d'angle } \frac{2\pi}{n} \\ \sigma = \text{symétrie par rapport à } D\left(\frac{\pi}{n}\right) \end{cases}$

σ est une symétrie orthogonale fixée.
Soit σ' une autre symétrie conservant le polygone régulier

$\sigma^{-1}\sigma'$ = rotation ~~d'angle~~ r conservant le polygone.

d'où $\sigma' = \sigma r$

-

~~(4) $D(G) = ([G,G])$ = groupe engendré par $x^{-1}y^{-1}xy = [x,y]$ = commutateur de $x, y \in G$. Remarquons que $[x,y]^{-1} = [y,x]$~~

~~a) $D(G) \triangleleft G$~~

~~$\forall y \in D(G)$~~

~~$\forall x \in G \qquad x^{-1}yx = y\,(y^{-1}x^{-1}yx) \in D(G)$~~

~~Si $H \triangleleft G$, alors $G/_H$ commutatif $\Leftrightarrow DG \subset H$~~

à enlever ainsi que feuille TD n° 1 et 2

× ① On dit que G est <u>résoluble</u> si il existe des sous groupes H_i tels que $\{e\} = H_0 \subset \dots \subset H_s = G$, $H_i \triangleleft H_{i+1}$ (cf ④ feuille 1) et H_{i+1}/H_i <u>abélien</u>.

a) Montrer que G résoluble, H sous groupe de G $\Rightarrow$ H résoluble. et si $H \triangleleft G$, G/H est resoluble (2 façons)

b) Soient (i, j, k, r, s) 5 entiers distincts, $\sigma = (i, j, k)$, $\tau = (k, r, s)$ des permutations circulaire montrer que $(k, j, s) = \sigma^{-1}\tau^{-1}\sigma\tau$.

c) En deduire que si $N \triangleleft H$ sous groupes de $\mathfrak{S}_n$, H/N etant abelien, et si H contient tous les 3-cycles ; ceux ci sont dans N

En deduire que si $n \geqslant 5$ $\mathfrak{S}_n$ n'est pas resoluble.

× ② Calculer l'ordre de $\sigma = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15 \\ 3, & 15, & 11, & 6, & 5, & 13, & 14, & 1, & 4, & 2, & 12, & 8, & 9, & 7, & 10 \end{pmatrix}$

(ie $n = \inf\{p / \sigma^p = 1\}$)

à conserver.

× ③ Soit $f : A \to A'$ un homomorphisme de groupe abelien $B \subset A$ un sous groupe d'indice fini noté ~~B : A~~ $(A : B)$

Montrer que ~~(B : A)~~ $(A : B) = (f(A) : f(B))(\ker f : \ker f|_B)$

× ④ • Soient G un groupe abelien et H, H' des sous groupes montrer que $\dfrac{H + H'}{H'}$ et $\dfrac{H}{H \cap H'}$ sont isomorphes

• Soit $0 \to G' \to G^+ \to G'' \to 0$ une suite exacte de groupes (~~abeliens~~) montrer que G^+ fini $\Leftrightarrow$ G' et G'' finis et qu'alors :

$$\# G^+ = \# G' \cdot \# G''.$$

(*)

× ⑤ On dit que la suite exacte $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ est <u>scindée</u> si il existe $s : G'' \to G$ telle que $g \circ s = Id_{G''}$

Montrer que les conditions equivalentes sont :

. il existe $G \xrightarrow{t} G'$ telle que $t \circ f = Id_{G'}$

. il existe un sous groupe H de G tel que $G = G' \oplus H$

(et alors $G'' \cong H$)

(*) • $H \triangleleft K_1 \triangleleft K_2$ $\left(K_1' = K_1/_H\right) \triangleleft \left(K_2' = K_2/_H\right)$ et $K_2'/_{K_1'} \simeq K_2/_{K_1}$

Si $H \triangleleft G$

a) G résoluble $\Leftrightarrow$ H et G/H sont résolubles.

($\Rightarrow$) ⓐ $0 \subset H_1 \cap H \subset \dots \subset H_n \cap H = H$

$H_i \cap H \triangleleft H_{i+1} \cap H$

$\left.\begin{array}{l} y \in H_i \cap H \\ x \in H_{i+1} \cap H \end{array}\right\} \Rightarrow x^{-1} y x \in H_i \cap H$

et $\dfrac{H_{i+1} \cap H}{H_i \cap H}$ abélien $\left\{\begin{array}{l} x \in H_{i+1} \cap H \\ y \in H_{i+1} \cap H \end{array}\right.$

$x^{-1} y^{-1} x y \in H_i \cap H \Rightarrow \dfrac{H_{i+1} \cap H}{H_i \cap H}$ commutatif.

(c.à.d $[\dot{x}, \dot{y}] = \dot{e}$)

ⓑ
préliminaire

On a : $D(G/H) \simeq D(G)/DG \cap H$

α' est la restriction de $\alpha : G \to G/H$

α' surjective

$$D(G) \xrightarrow{\alpha'} D(G/H) \subset G/H$$

$$[x, y] \longmapsto [\dot{x}, \dot{y}] = \dot{\overline{[x, y]}}$$

$$\downarrow$$

$$D(G)/\operatorname{Ker}\alpha' \xrightarrow[\simeq]{\alpha'} D(G/H)$$

or $\operatorname{Ker}\alpha' = D(G) \cap H$ ($= \operatorname{Ker}\alpha \cap D(G)$) et $DG \cap H$ distingué

$$\boxed{D(G/H) \simeq D(G)/DG \cap H}$$

$$D(G/H) \simeq D^2(G)/D^2G \cap (DG \cap H) \simeq D^2(G)/D^2G \cap H$$

Par récurrence : $\boxed{D^i(G/H) \simeq D^i(G)/D^iG \cap H}$

montrons que G/H résoluble dès que G résoluble

$$\exists r \,/\, D^r(G/H) \simeq D^r(G)/_{D^r G \cap H} = \{e\}/_{\{e\}\cap H} = \{e\}$$

($\Leftarrow$) Réciproquement, G/H résoluble $\Rightarrow$ $D^r(G)/_{D^r(G)\cap H} = \{e\}$

d'où $D^r(G) \subset H$. H résoluble $\Rightarrow \exists r' \,/\, D^{r'}(H) = \{e\}$

d'où $D^{r'+r}(G) \subset D^{r'}(H) = \{e\} \Rightarrow D^{r'+r}(G) = \{e\}$

ce qui montre que ~~$D^{r'+r}(G)$~~ G est résoluble.

Autre démonstration :

$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_s = H$

$G' = G/H$

$\{e\} = H'_s \subset H'_{s+1} \subset \ldots \subset H'_{s+t} = G'$

Il y a une bijection croissante de l'ensemble des sous-groupes de G/H dans l'ensemble des sous-groupes de G qui contiennent H.

$H'_i \subset G' = G/H$

Il existe H_i sous-groupe de G tel que $H \subset H_i \subset G$

et $H'_i = H_i/H$ $\quad$ ($H \triangleleft H_i$ car $H \triangleleft G$)

Alors :

$e = H_0 \subset \ldots \subset H_s = H \subset H_{s+1} \subset \ldots \subset H_{s+t} = G$

Remarque :

$G' = G/H$ où $H \lhd G$

Il existe une bijection

$\{K' \,/\, K' \subset G', \text{sous-groupe de } G'\} \longrightarrow \{K \subset G \text{ sous-groupe tel que } K \supset H\}$

de plus, K distingué ssi K' distingué.

preuve :

On prend $K' \longrightarrow \varphi^{-1}(K') = \{x \in G \,/\, \dot{x} = \varphi(x) \in K'\} = K$

$$K/H \xleftarrow{\ \varphi\ } K$$

$\begin{cases} \varphi(\varphi^{-1}(K')) = K' & \text{donc } \varphi \text{ surjective.} \\ \varphi^{-1}(\varphi(K)) \supset K & \text{. On a l'égalité, car :} \end{cases}$

$x \in \varphi^{-1}(\varphi(K)) \iff \varphi(x) \in \varphi(K) \iff \exists y \,/\, \varphi(x) = \varphi(y) \ y \in K$

$\iff \varphi(xy^{-1}) = e \ \ \underline{y \in K} \iff \underline{xy^{-1} \in H \subset K}$

$\iff$ d'où $x \in K$.

Ici $\varphi^{-1}(\varphi(K)) = K$

$K/H = K'$

Thm 1) $\underline{K \lhd G \quad H \subset K \subset G \implies K' \lhd G'}$

$\dot{x} \in G'$
$\dot{y} \in K'$ $\quad \dot{x}^{-1}\dot{y}\dot{x} = \overline{x^{-1}yx}$ où $y \in K$ et $x \in G$

comme $x^{-1}yx \in K \implies \dot{x}^{-1}\dot{y}\dot{x} \in K'$ donc K' distingué.

2° $K' \triangleleft G' \Rightarrow K \triangleleft G$

$y \in K$ $\quad x^{-1}yx \quad \overline{x^{-1}yx} = \dot{x}^{-1}\dot{y}\dot{x} \in K'$ car K' distingué.
$x \in G$

donc $x^{-1}yx \in K \Rightarrow K \triangleleft G$

② $\sigma = (1,3,11,12,8) \circ (2,15,10) \circ (4,6,13,9) \circ (5) \circ (7,14)$

$$\sigma^n = \prod_{i=1}^{k} \sigma_i^n$$

$\sigma^n|_{E_i} = \sigma_i$ donc $\sigma^n = Id \Leftrightarrow \sigma_i^n = Id \quad i = 1, \dots, k$

$\Updownarrow$

$\forall i \; n_i | n$ où n_i = ordre de σ_i

$\Updownarrow$

$ppcm(n_1, \dots, n_k) | n$

l'ordre de σ est le $ppcm(n_1, \dots, n_k)$.

Ici : $ppcm(5,3,4,2) = 60$

Remarque : $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k$ dans S_8

$n_1 \geq \dots \geq n_k$

$n_1 = 8$	ordre de $\sigma = 8$
7	7
6	6
5	(15)
4	12
3	3

(4) 1°/ $(H+H')/_{H} \simeq H/_{H\cap H'}$

La suite $0 \longrightarrow H\cap H' \overset{\alpha}{\hookrightarrow} H \overset{\beta}{\longrightarrow} H+H'/_{H'} \longrightarrow 0$ est exacte.

$x \longmapsto \alpha(x)=x$

$x \longmapsto \dot{x}_{H'}$

Remarque : Montrer que si $H \triangleleft G$ (non forcément commutatif), on a :

1) HH' est un sous-groupe de G.

2) $HH'/_{H} \simeq H/_{H\cap H'}$

2°/ $0 \longrightarrow G' \overset{\alpha}{\longrightarrow} G \overset{\beta}{\longrightarrow} G'' \longrightarrow 0$

$\alpha : G' \to \alpha(G') \subset G$, $G \to G/_{\alpha(G')}$, $\bar{\beta} : G/_{\alpha(G')} \to G''$

1) G fini $\Leftrightarrow$ G' et G'' finis

$\alpha(G') = \ker\beta$ sous-groupe distingué de G.

$\bar{\beta}$ est un isomorphisme de groupes.

Donc $G'' \simeq G/_{\alpha(G')}$ (1)

(1) : G fini $\Rightarrow$ $\alpha(G')$ fini et G'' fini

$\Updownarrow$ (car $\alpha : G' \xrightarrow{\sim} \alpha(G')$)

G' fini et G'' fini.

Inversement, si G' et G'' sont finis, alors $G/_{\alpha(G')}$ fini et $\alpha(G')$ fini.

Ainsi $G = \bigsqcup_{\alpha \in G/_{\alpha(G')}} \pi^{-1}(\alpha)$ où π est la surj. can. de G sur $G/_{\alpha(G')}$.

($G/_{\alpha(G')}$ fini ; $\pi^{-1}(\alpha)$ fini, de cardinal $|\alpha(G')|$)

donc G est fini.

2) $\# G = \# G' . \# G''$

Si G est fini, $G'' \simeq G/_{\alpha(G')} \Rightarrow \# G'' = \dfrac{\# G}{\# \alpha(G')} = \dfrac{\# G}{\# G'}$

CQFD

③ On utilise le ④.

$$0 \longrightarrow \ker f / \ker f|_B \xrightarrow{\varphi} A/B \xrightarrow{\psi} f(A)/f(B) \longrightarrow 0 \qquad (1)$$

$$\tilde{x} \longmapsto \dot{x} = \dot{\overline{x+b}}$$

$$\dot{x} \longmapsto \overline{f(x)}$$

- φ et ψ sont bien définies : $\tilde{x} = \tilde{y} \Leftrightarrow x - y \in \ker f|_B = B \cap \ker f$
  $\Rightarrow \dot{x} = \dot{y}$
  et $\dot{x} = \dot{y} \Leftrightarrow x - y \in B \Rightarrow f(x) - f(y) \in f(B)$
  cad $\overline{f(x)} = \overline{f(y)}$

- (1) est une suite exacte :

$$* \begin{cases} \ker \psi = \{\dot{x} \in A/B \ / \ f(x) \in f(B)\} \\ \operatorname{Im} \varphi = \{\dot{x} \in A/B \ / \ \exists b \in B \quad x + b \in \ker f\} = \{\dot{x} \in A/B \ / \ f(x) \in f(B)\} \end{cases}$$

* φ injective : $\dot{x} = 0 \Leftrightarrow x \in B$
or $x \in \ker f \Rightarrow x \in B \cap \ker f = \ker f|_B \Rightarrow \tilde{x} = 0$

* ψ surjective : évident.

D'après le ③ : $\ker f / \ker f|_B$ et $f(A)/f(B)$ sont finis et :

$$\boxed{[A : B] = [f(A) : f(B)] \times [\ker f : \ker f|_B]}$$

(5) **Def** | $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ scindée si $\exists s : G'' \to G$ telle que $g \circ s = Id_{G''}$
(suite exacte)

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$$
($t : G \to G'$, $s : G'' \to G$) $g \circ s = Id_{G''}$

Montrer que Def $\Leftrightarrow$ 1) $\Leftrightarrow$ 2) où :

1) $\exists t : G \to G' \,/\, t \circ f = Id_{G'}$

2) $\exists H$ sous-groupe de G tel que $G = G' \oplus H$ (et alors $G'' \simeq H$)

Def $\Rightarrow$ 1) Soit $x \in G$ $t(x)$?

$g(x) = x''$ $g \circ s(x'') = x''$ $\Rightarrow$ $x - s(x'') \in \operatorname{Ker} g = \operatorname{Im} f$

Posons $x - s(x'') = f(\xi)$ et prenons $\xi = t(x)$.

t est bien définie.

Il nous faut vérifier que a) t est un homomorphisme

b) ~~$f \circ t = Id_G$~~ $t \circ f = Id_{G'}$

a) Soit $x + y \in G$ $g(x+y) = (x+y)'' = x'' + y''$

et $g \circ s(x'' + y'') = x'' + y''$

Donc $x + y - s(x'' + y'') \in \operatorname{Ker} g = \operatorname{Im} f$

et, en égard à notre définition de t : $x + y - s(x'' + y'') = f(t(x+y))$

d'où $\underbrace{[x - s(x'')]}_{f(t(x))} + \underbrace{[y - s(y'')]}_{f(t(y))} = f(t(x+y))$

Comme f est un homomorphisme : $f(t(x) + t(y)) = f(t(x+y))$

Comme f est injective : $t(x+y) = t(x) + t(y)$

b) $t \circ f = Id_{G'}$?

Soit $x' \in G'$ $f(x') \in G$

$\begin{cases} g(f(x')) = 0 \\ g \circ s(0) = 0 \end{cases}$ $\Rightarrow$ $f(x') - s(\underbrace{g \circ f(x')}_{0}) \in \operatorname{Ker} g = \operatorname{Im} f$

et $f(x') = f(t(f(x')))$ $\underset{f \text{ inj}}{\Rightarrow}$ $x' = t \circ f(x')$

Ce qui prouve que $t \circ f = Id_{G'}$

1) ⇒ 2)

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0 \quad (t : G \to G')$$

$f(G') \simeq G'$ car f est injective.

Soit $H = \ker t$

Alors $\boxed{G = f(G') \oplus \ker t}$

[En effet : • $x \in f(G') \cap \ker t$ $\begin{cases} t(x) = 0 \\ x = f(x') \end{cases}$ $\Rightarrow t \circ f(x') = x' = 0 \Rightarrow x = 0$

• $\forall x \in G$ $\quad x = \underbrace{f(t(x))}_{\in f(G')} + \underbrace{(x - f(t(x)))}_{\ker t} \Rightarrow G = f(G') + \ker t$]

2) ⇒ Déf On suppose que $G = f(G') \oplus H$. Comme $f(G') = \ker g$,

$G = \ker g \oplus H$

$$G \xrightarrow{g} G'' \to 0 \quad (s : G'' \to G)$$

$\forall x'' \in G''$ $\exists !\, x \in H$ $g(x) = x''$ $\quad$ (cf. $g(x) = g(y) \Leftrightarrow x - y \in H \cap \ker g = \{0\}$) $\quad$ $x, y \in H$

Posons $s(x'') = x$

Alors : s est un homomorphisme et $g \circ s(x'') = g(x) = x''$. CQFD

---

exercice supplémentaire : Sur $G' \times G'' = G$

$$(x', x'')(y', y'') = (x' \alpha_{x''}(y'), x'' y'')$$ (produit semi-direct)

* c'est une loi de groupe

* On a une suite exacte scindée

$$0 \to G' \to G \to G'' \to 0$$

(où $G'' \to \operatorname{Aut} G'$, $x'' \mapsto \alpha_{x''}$ est un homomorphisme)

Remarque 1 : $0 \to A_n \to \mathfrak{S}_n \xrightarrow{\varepsilon} \{-1, +1\} \to 0$ $\quad (s)$

est sciendée (siouxdée)

$s(+1) = Id$

$s(-1) = \tau$ transposition.

Remarque 2 :

$$0 \longrightarrow O^+(2) \longrightarrow O(2) \longrightarrow \{\pm 1\} \longrightarrow \{1\}$$

$$s(x,y) = (-x,y)$$

× ① a) Montrer que si $p \in \mathbb{N}$ est premier $\mathbb{Z}/p\mathbb{Z}$ est un corps (noté K)

b) Ainsi $(\mathbb{Z}/p\mathbb{Z} - \{\dot{0}\})$ est un groupe pour la multiplication
on se propose de montrer que ce groupe est cyclique :

(i) Soit $(p-1) = q_1^{\beta_1} \cdots q_s^{\beta_s}$ une decomposition en facteur irreductible, montrer que $\forall x \in K - \{\dot{0}\}$ $x^{p-1} = 1$

(ii) $\frac{p-1}{q_i} \in \mathbb{N}$ est inferieur strictement à $p-1$; en deduire l'existence de $x_i \in K - \{\dot{0}\}$ non racine de $X^{p-1/q_i} - 1$
(i.e $x_i^{(p-1)/q_i} \neq 1$)

(iii) En conclure que $y_i = x_i^{(p-1)/q_i^{\beta_i}}$ est d'ordre $q_i^{\beta_i}$ dans $(K - \{0\})$
puis que $y_1 \cdots y_s = y$ engendre K.

(NB. Ulterieurement on montrera peut-être que tout corps fini est commutatif d'ordre p^n, p premier et que $K - \{0\}$ est cyclique.)

×' ② Soit G un groupe commutatif fini, noté multiplicativement
$n \in \mathbb{N}$ tel que $\forall x \in G$ $x^n = e$

a) Soit $n = rs$, r, s premier entre eux.
- $M = \{x \in G \mid x^r = e\}$, $N = \{x \in G \mid x^s = e\}$
sont des sous groupes de G.
- Montrer que $M \times N \longrightarrow G$ est un isomorphisme.
$(x, y) \longrightarrow xy$

b) Soit $n = p_1^{r_1} \cdots p_k^{r_k} = q_1 \cdots q_k$, p_i premier, la decomposition en facteurs irreductible de n. $q_i = p_i^{r_i}$. Alors
G est isomorphe au produit direct des $M_i = \{x, x^{q_i} = e\}$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| $
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad G(p_i)$

c) Soit G un groupe comm. fini $r \in \mathbb{N}$, p premier tel que : $\forall x \in G \quad x^{p^r} = e$.

Montrer que $\# G$ est une puissance de p.

d) En déduire que si $\# G = n = p_1^{r_1} \cdots p_h^{r_h}$, p_i premiers distincts, G est isomorphe au produit direct de h groupes d'ordre $p_i^{r_i}$

---

③ $(G,+)$ groupe commutatif muni d'une relation d'ordre $\leq$ est dit ordonné si : $\forall x, y, z \in G$

$$x \leq y \Rightarrow x+z \leq y+z$$

1) Montrer que G est ~~ordonné~~ (un groupe ordonné) $\Longleftrightarrow$ $P + P \subseteq P$ et $P \cap (-P) = \{0\}$

tel que $P = \{x \,/\, x \geq 0\}$

2) Décrire P lorsque $\leq$ est l'ordre lexicographique (resp. l'ordre produit sur $\mathbb{Z}^2$ (vérifier que ces ordres munissent G d'une structure de groupe ordonné)

3°) L'ordre est total ssi $P \cup (-P) = G$.

4°) Déterminer toutes les structures de groupe ordonné sur un groupe cyclique (fini, c'est trivial, ou infini c'est plus intéressant...)

④ Soit A un sous groupe de G.

on note $N(A) = \{ g \in G \quad g^{-1} A g = A \}$ normalisateur de A

$$Z(A) = \{ a \in A, \ \forall a' \in A \quad aa' = a'a \}$$

montrer que ~~Z(A)~~ $N(A)$ et $Z A$ sont des sous groupes de G et que $Z(A) \triangleleft N(A)$ ($A \triangleleft N(A)$ aussi !).

~~⑤ Interpréter $N(A)$ en termes de l'action de G sur lui même~~

~~$G \times G \longrightarrow G$~~

~~$g, g' \longrightarrow \sigma(g)(g') = g g' g^{-1}$~~

~~(Montrer que $N_x = \{ g \in G \quad x g x^{-1}$ est [illegible] $\}$ est un sous groupe)~~

(1) a) facile (connu !) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps.

b) i) facile

ii)

$$p-1 = q_1^{\beta_1} \cdots q_s^{\beta_s} \quad \beta_i > 0 \ ; \ q_i \in \mathcal{P}$$

$$\exists x_i \in G = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \quad / \quad x_i^{\frac{(p-1)}{q_i}} \neq 1$$

Le polynôme $X^{\frac{p-1}{q_i}} - 1$ a au plus $\frac{p-1}{q_i} < p-1$ racines. Comme $\# G = p-1$, l'existence de x_i est prouvée.

iii) $y_i = x_i^{\frac{p-1}{q_i^{\beta_i}}}$

- $y_i^{q_i^{\beta_i}} = 1 \Rightarrow \omega(y_i) \mid q_i^{\beta_i} \Rightarrow \omega(y_i) = q_i^{\alpha_i} \quad \alpha_i \leq \beta_i$

Si $\alpha_i < \beta_i$, on aurait $y_i^{q_i^{\beta_i - 1}} = 1$.

Ici, nous avons $y_i^{q_i^{\beta_i-1}} = x_i^{\frac{p-1}{q_i^{\beta_i}} q_i^{\beta_i-1}} = x_i^{\frac{p-1}{q_i}} \neq 1$, donc ~~⇒~~ $\alpha_i = \beta_i$

Ainsi : $\boxed{\omega(y_i) = q_i^{\beta_i}}$ dans $G \setminus \{0\}$

~~iiii)~~ On prend $y = y_1 \cdots y_s$

- $y^{\frac{p-1}{q_i}} \neq 1$ pour tout i, de sorte que $\omega(y) = p-1$.

Montrons que $y^{\frac{p-1}{q_i}} \neq 1$

$$y^{\frac{p-1}{q_i}} = \underbrace{y_1^{\frac{p-1}{q_i}}}_{= 1} \cdots y_i^{\frac{p-1}{q_i}} \cdots \underbrace{y_s^{\frac{p-1}{q_i}}}_{= 1}$$

1 car $\omega(y_s) = q_s^{\beta_s} \mid \frac{p-1}{q_i}$

$$y^{\frac{p-1}{q_i}} = y_i^{\frac{p-1}{q_i}} \neq 1 \text{ car } q_i^{\beta_i} \nmid \frac{p-1}{q_i} \quad (\text{où } q_i^{\beta_i} = \omega(y_i))$$

Conclusion : y engendre $(\mathbb{F}_p \setminus \{0\}, \times)$

Remarque : 1) $x, y \in G$ G est un groupe d'ordre n.

$$\omega(x \cdot y) = \omega(x)\,\omega(y) \text{ si } \Delta(\omega(x), \omega(y)) = 1.$$

2) K corps fini. $\{n.1 \,/\, n \in \mathbb{Z}\} \simeq \mathbb{F}_p$ où p = caractéristique du corps K. $\mathbb{F}_p \subset K$ K est donc un sur corps de $\mathbb{F}_p$, il peut être considéré comme un ev sur $\mathbb{F}_p$: $K \simeq (\mathbb{F}_p)^r$

Ainsi $\# K = p^r$ et $\dim_{\mathbb{F}_p} K = r$

• Il existe, à isomorphisme près, un unique corps $\mathbb{F}_{p^r}$; $\# \mathbb{F}_{p^r} = p^r$; et $K \setminus \{0\}$ est un groupe cyclique.

Exercice

Déterminer les groupes à 8 éléments. ($8 = 2^3$) (à isomorphisme près)

Solution : $n = \# G = 8$

$p = \# Z(G) = 2$ ou 4 ou 8 (car $\# Z(G) \equiv 0 \, [p]$ si G = p-groupe)

• $p = 8$: G est commutatif, donc de la forme $\mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

• $p = 4$: $Z(G) = \{e = x_0, x_1, x_2, x_3\}$

$G = \{e, x_1, x_2, x_3\} \cup \{g, gx_1, gx_2, gx_3\}$ où $g \notin Z(G)$

Alors $gx_1 gx_2 = g^2 x_1 x_2 = g^2 x_2 x_1 = gx_2 gx_1$

et la loi est commutative dans G ! Ce qui est absurde.

Ce cas est impossible.

• $p = 2$:

$$0 \to Z(G) \hookrightarrow G \to G/Z(G) \to 0 \quad \text{est exacte.}$$

$\# G/Z(G) = 4$ et il n'y a que 2 types de groupes à 4 éléments (tous commutatifs). De 2 choses l'une :

* Si $G/Z(G) \simeq \mathbb{Z}/4\mathbb{Z}$, soit $a \in G$ / $\bar{a}$ engendre $G/Z(G)$.

$\omega(a) = 4$ ou 8. Ce ne peut être 8 car sinon G commutatif.

Donc $\omega(a) = 4$, et on peut scinder la suite ($\leftarrow - - -$)

$$(a) \xrightarrow{\sim} G/Z(G)$$

Alors $\forall g \in G \; \exists! \, z \in Z(G) \, \exists! \, i \in [0,1,2,3]$ / $g = za^i$

(puisque suite scindée $\Rightarrow$ $G = Z(G) \times G/Z(G)$, ou $Z(G) \triangleleft G$)

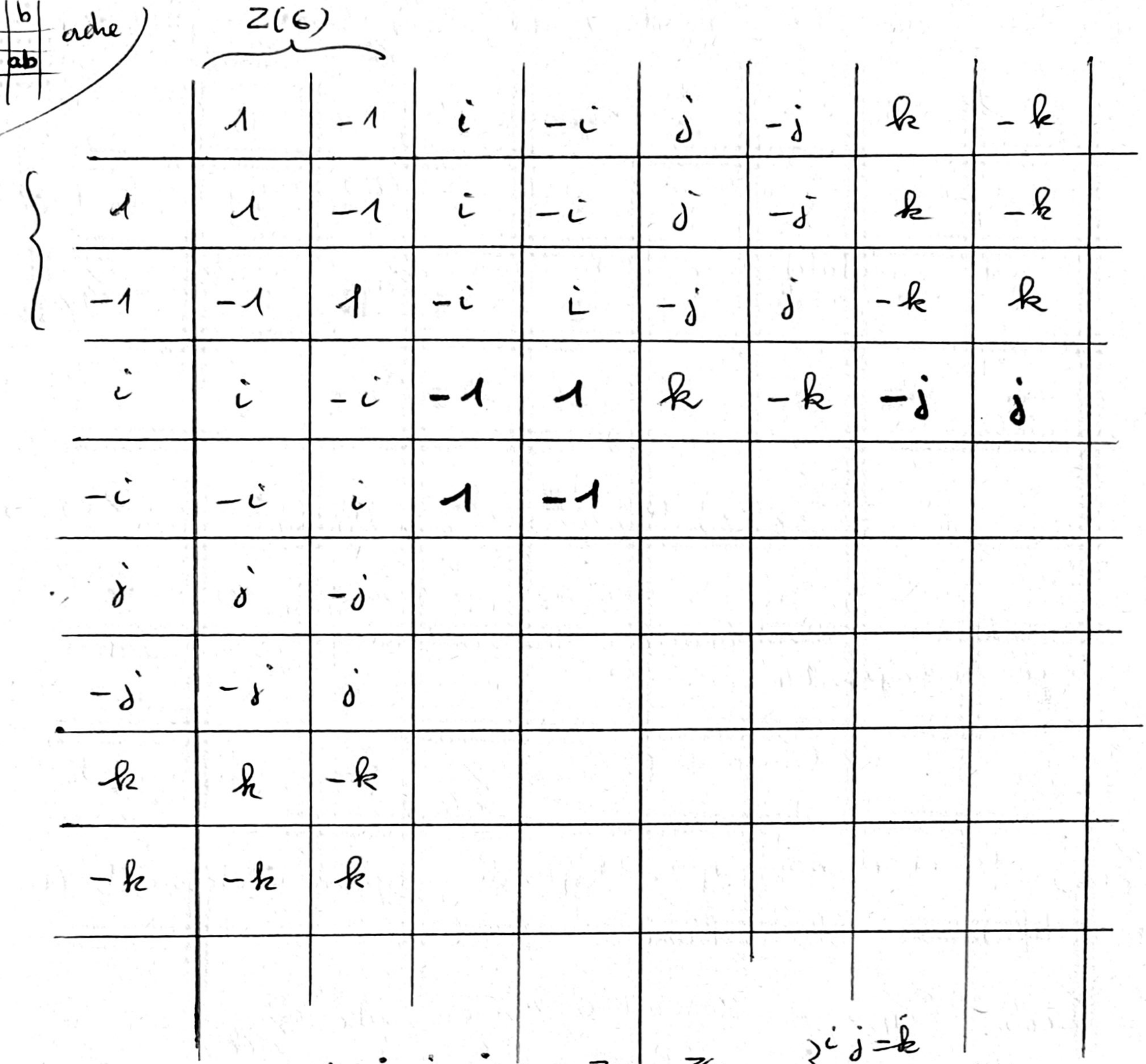
(En effet : $\bar{g} = \bar{a}^i \Rightarrow g = a^i z$ où $z \in Z(G)$).)

Donc $\underline{G \text{ est commutatif}}$ $[(za^i)(z'a^j) = (z'a^j)(za^i)$ car $z, z' \in Z(G)]$

Ce qui est absurde. Donc :

* $G/Z(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

a | b | ab — ache



$Z(G)$	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	**-1**	**1**	k	-k	**-j**	**j**
-i	-i	i	**1**	**-1**				
j	j	-j						
-j	-j	j						
k	k	-k						
-k	-k	k						

On a : $G/_{Z(G)} = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow \begin{cases} \bar{i}\bar{j} = \bar{k} \\ \bar{i}^2 = \bar{j}^2 = \bar{k}^2 = \bar{1} \end{cases}$

<u>on peut supposer</u> que $ij = k$ (c'est la structure de $G/_{Z(G)} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui nous le donne $\exists$: $ij = \pm k$, ...)

$\bar{i}^2 = \bar{0} \Leftrightarrow i^2 \in Z(G) = \{1, -1\}$. <u>Si $i^2 = 1$</u>, alors

~~$\{1, i, j, k\}$ est un sous-groupe de G car :~~

~~$i^2 = 1$~~

~~$j = ik$~~

~~$ij = k$~~

On veut montrer que $\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k \\ jk = i \\ ki = j \end{cases}$

Si $i^2=j^2=k^2=1$, alors $ij=k \Rightarrow ij=ji$ etc et G commutatif.

On peut donc supposer que $\boxed{i^2=-1}$.

(autre façon de le voir : Si tout élément de G est d'ordre 2, alors G est commutatif.
En effet : ~~$abba=ab^2a=aa=a^2=1$ d'où~~ ~~$abba=1 \Rightarrow abb=a$~~
~~$a^2=1$ $b^2=1$ alors $(ab)^{-1}=b^{-1}a^{-1}$~~ $=ba$
et $abba=1 \Rightarrow (ab)^{-1}=ba \Rightarrow ab=ba$ } $\Rightarrow ba=ab$)
$\parallel$
ab car $(ab)^2=1$

$G/_{Z(G)} \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$

Soit $i \in G$ d'ordre 4 $\bar{i} \neq 1$ $i^2 \in Z(G)=\{\pm 1\} \Rightarrow \underline{i^2=-1}$

$G/_{Z(G)} = (1, \bar{i}, \bar{j}, \bar{k})$ $ij=k$

● 1^er^ cas $j^2=1$ * Si $k^2=1$, ~~on tombe sur une contradiction~~ on trouve D_4. En effet : on construit la table :

~~$ij=k \Rightarrow kj=i$~~
~~$ij=k \Rightarrow ik=-j$~~
~~$ji=-k$ et $jk=...$~~

$$\begin{cases} kj=i & jk=-i \\ ik=-j & ki=j \\ ij=k & ji=-k \end{cases}$$

On a la table du groupe : c'est le groupe diédral D_4, ou "groupe du carré".

$rot(\frac{\pi}{2})=i$

j

$ij=k$

● * Si $k^2=-1$, on tombe sur une contradiction.

On a :
$$\begin{cases} i^2=-1 \\ j^2=1 \\ k^2=-1 \end{cases} \quad ij=k$$

$jk=i$	$kj=i$
$ik=-j$	$ki=-j$
$ij=k$	$ji=k$

donc i,j,k commutent entre eux. On tombe sur G commutatif. Absurde puisque $\#Z(G)=2$.

2^e^ cas $j^2=-1$ * si $k^2=-1$, on a
$$(*) \begin{cases} i^2=j^2=k^2=-1 \\ ij=k \quad jk=i \quad ki=j \\ ji=-ij \quad jk=-kj \quad ki=-ik \end{cases}$$

on écrit que G est isomorphe au groupe des quaternions : $Q=\mathbb{R}^4$ muni d'une multiplication donnant $(*)$:
$(x+yi+zj+tk)(x'+y'i+z'j+t'k)$ = à développer. Q = corps des quaternions.

Exercice : Soit $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} / a, b, c \in K \text{ corps} \right\}$ Montrer que G est un groupe pour x, et que $M_{a,b,c} \in Z(G) \Leftrightarrow a = b = 0$.

Vérifier que $G/Z(G)$ est commutatif (ind : $M_{a,b,c} \in M_{a,b,0} Z(G)$)

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a'+a & c'+ab'+c \\ 0 & 1 & b'+b \\ 0 & 0 & 1 \end{pmatrix}$$

la loi est interne. Cherchons l'inverse de M_{abc} :

$$\begin{cases} a'+a=0 \\ c'+ab'+c=0 \\ b'+b=0 \end{cases} \Leftrightarrow \begin{cases} a'=-a \\ b'=-b \\ c'=-c+ab \end{cases}$$

existe et est unique et $\in G$.

él. neutre : Id.

Centre de G ? On cherche (a,b,c) tels que $\forall a', b', c'$ on ait :

$$\begin{cases} a'+a = a+a' \\ \cancel{c'} + ab' + c = c + a'b + \cancel{c'} \\ b'+b = b+b' \end{cases} \Leftrightarrow a'b + b'(-a) = 0$$

$\forall a', b', c'$

$\Updownarrow$

$b = a = 0$

cqfd

(1) Soit G un groupe d'ordre p^k, ~~$p>0$~~ p premier

a) montrer que $Z(G) \neq \{e\}$ ($Z(G)$ centre de G)

b) Montrer que tout groupe d'ordre p^2 est commutatif

(2) Un groupe est simple si $H \lhd G$ implique $H = \{e\}$ ou G

Montrer qu'un groupe d'ordre 220 admet un seul 11-groupe de Sylow. En déduire que G n'est pas simple.

Montrer qu'un groupe d'ordre 15, 20, 30, 48, 36, 96, 160, 56 ou $p^2 m$ ($p^2 > m$, p premier) n'est pas simple

(3) Deduire de (1) a) que tout groupe d'ordre p^k est non-simple ~~($k>1$)~~ dès que $k > 1$

(4) a) Soit G un groupe opérant transitivement sur un ensemble E

Montrer l'équivalence des deux propriétés i) et ii) suivantes

(i) Tout stabilisateur H_x est un sous groupe maximal.

(ii) Si $F \subset E$ satisfait à $\forall g \in G \ (g.F \subset F$ ou $g(F) \cap F = \emptyset)$ alors $F = E$ ou $\# F = 1$.

un tel G est dit primitif

b) G est dit r transitif sur E si :

(P_r) quel que soient $(a_1, \dots, a_r)$; $(b_1, \dots ; b_r)$ dans E, avec $a_i \neq a_j$, $b_i \neq b_j$ si $i \neq j$; il existe $\sigma \in G$ tel que $\sigma(a_i) = b_i$.

~~et si (P_{r+1}) n'est~~

Montrer que :

- $P_r \Rightarrow P_{r-1}$
- $\mathfrak{S}_n$ est n-transitif, A_n $n-2$ transitif
- $r>1 \Rightarrow G$ est primitif

$G \subsetneq \mathfrak{S}_E$.

c) Soit G primitif, $N \triangleleft G$ sous groupe normal propre alors N est transitif. (considérer $F = N.x$ pour tous les $x \in E$)

d) On veut montrer que A_5 est simple :
Soit $1 \neq N \triangleleft A_5$. Montrer que N contient un sous groupe cyclique engendré par $(1, 2, 3, 4, 5) = \sigma$

- $\tau = (1, 2, 3)$ montrer que $\tau \sigma \tau^{-1} \neq \sigma$
En déduire que N contient 6 5-sous groupe de Sylow.

- Montrer que si $\# N = 30$, N contient 24 éléments d'ordre 5, en déduire une contradiction.

(5) On désigne par $\hat{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$ l'ensemble obtenu en complétant $\mathbf{C}$ par un «point à l'infini». On appelle *homographie* l'application f de $\hat{\mathbf{C}}$ dans lui-meme définie par les nombres complexes a, b, c, d, $ad-bc \neq 0$ telle que:

$$c \neq 0 \quad \begin{cases} f(z) = \dfrac{az+b}{cz+d} & \text{si } z \neq \infty \text{ et } z \neq -\dfrac{d}{c} \\ f(\infty) = \dfrac{a}{c}, & f\left(-\dfrac{d}{c}\right) = \infty \end{cases}$$

$$c = 0 \quad \begin{cases} f(z) = \dfrac{a}{d} z + \dfrac{b}{d} & \text{si } z \neq \infty \\ f(\infty) = \infty. \end{cases}$$

Si les points invariants sont distincts, l'homographie sera dite *non parabolique* (*parabolique* dans le cas contraire).

Question 1. — Montrer que l'ensemble G des homographies est un groupe (dit *circulaire*), opérant sur $\hat{\mathbf{C}}$ et que l'ensemble H des homographies vérifiant $ad-bc = 1$ est un sous-groupe de G.

Question 2. — *a)* Montrer qu'une homographie parabolique, distincte de l'identité, engendre dans H un sous-groupe cyclique infini.

b) Soit Γ un sous-groupe fini de H. Montrer que si tous les éléments de Γ ont même point invariant α alors Γ est un groupe cyclique. En déduire que tous les éléments de Γ ont mêmes points invariants.

Question 3. — Soit Γ un sous-groupe fini d'ordre n de H. On dira que $x \in \hat{\mathbf{C}}$ est un *pôle* de Γ s'il existe un élément f de Γ, distinct de l'identité, tel que $f(x) = x$.

a) Montrer que l'ensemble des pôles $\mathcal{P}$ de Γ est un Γ-ensemble. ($x \in \Gamma$ opère sur $\mathcal{P}$)

b) Soit L_x et H_x l'orbite et le stabilisateur de x, pôle de Γ et η_x et ν_x leurs cardinaux. Etablir la relation:

$$2 - \frac{2}{n} = \sum_{L_x} \left(1 - \frac{1}{\nu_x}\right).$$

On pourra introduire le nombre de couples (f, x) où f est un élément de Γ, distinct de l'identité et où x est un pôle de f. En déduire qu'il ne peut y avoir que deux ou trois orbites.

Question 4. — Montrer que s'il n'existe que deux orbites, Γ est un groupe cyclique d'ordre n.

Question 5. — On suppose qu'il existe trois orbites dans le Γ-ensemble $\mathcal{P}$. On notera ν_1, ν_2, ν_3 les cardinaux des stabilisateurs avec $\nu_1 \leq \nu_2 \leq \nu_3$.

a) Montrer que $\nu_1 = 2$ et $2 \leq \nu_2 < 4$.

b) Si $\nu_2 = 2$, montrer que Γ est le groupe diedral D_{ν_3} des isométries planes qui laissent globalement invariant un polygône régulier de ν_3 sommets.

c) Si $\nu_2 = 3$, montrer que $n = 6k$ avec $k \geq 2$ et $\nu_3 = \dfrac{6k}{k+2}$, en déduire que n ne peut prendre que trois valeurs.

<u>Question d) TD</u>

Il existe $J \subset N$, J sous-groupe d'ordre 5 $\Rightarrow$ J cyclique $J = \langle \sigma \rangle$

Donc σ est d'ordre 5 dans $\mathcal{S}_5$, donc σ = permutation circulaire.

Ainsi, $\exists \sigma$ ordre 5 $\sigma = (1,2,3,4,5)$ $J = \langle\sigma\rangle \subset \mathcal{S}_5$.

$\tau = (1,2,3) \Rightarrow \tau J \tau^{-1} \neq J$

$\mathcal{S}$ = ensemble des 5-sous-groupes de Sylow de N

$$\left.\begin{array}{l} \left.\begin{array}{l} n = \# \mathcal{S} \\ n \equiv 1 \ [5] \end{array}\right\} \\ \text{et } n \mid \# N \mid 60 \Rightarrow n \mid 60 \end{array}\right\} \Rightarrow n = 6$$

• J_1, J_2, J_3, J_4, J_5, sont disjoints deux à deux

Donc N contient $4 \times 6 = 24$ éléments d'ordre 5. Comme $\# N = 5, 10, 15, 20, 30$ (cf. $(*) \Rightarrow 5 \mid \# N$, et $\# N \mid 60$) ou 60, on aura nécessairement :

$$\# N = 30 \text{ ou } 60$$

Supposons, par l'absurde, que $\# N = 30$. Alors N contient 6 éléments d'ordre ~~1, 2, 3 ou 6~~ différents de 5 ; notons les $1, a, b, c, d, e$.

• N opère sur $\{1,2,3,4,5\}$ $\quad \# N = \#(\text{orb}1)(\# H_1) = 5 . \# H_1 \quad (*)$

où $H_1 = \{ g \in N \ / \ g(1) = 1 \}$

$\# N = 30$ et $(*) \Rightarrow \# H_1 = 6$

Alors je dis (il dit) que $H_1 = \{1, a, b, c, d, e\}$. En effet, sinon $\exists$ el. d'ordre 5 dans $H_1 \Rightarrow \exists k$ $J_k \subset H_1$ absurde car $\left\{\begin{array}{l} \# J_k = 5 \\ \# H_1 = 6 \end{array}\right.$

Donc $H_1 = \{1, a, b, c, d, e\}$

On peut refaire ce développement (à partir de $(*)$). On obtient :

$$\left.\begin{array}{l} H_1 = H_2 = H_3 = H_4 = H_5 = \{1, a, b, c, d, e\} \\ \text{ce qui est absurde, puisque } H_1 \cap \ldots \cap H_5 = \{Id\} \end{array}\right\} \Rightarrow \{1, a, b, c, d, e\} = \{1\} \text{ absurde}$$

Conclusion : A_5 est simple

(1) Déterminer : - tous les sous anneaux de $\mathbb{Z}$, les systèmes libres, générateurs minimaux, toutes les bases.
- Même questions pour $\mathbb{Z}/p\mathbb{Z}$ considéré comme $\mathbb{Z}$-module

× (2) Soient A un anneau, M un A-module. (A commutatif)
- Déterminer $\mathrm{Hom}_A(A, M)$
- Soit $M^* = \mathrm{Hom}_A(M, A)$ { Munir M^* d'une structure de A-module ; Montrer qu'il existe une application naturelle $M \to M^{**}$, en général ni injective ni surjective.
déterminer $(\mathbb{Z}/p\mathbb{Z})^*$, $\mathbb{Z}/p\mathbb{Z}$ étant considéré comme un $\mathbb{Z}$-mod
(resp : comme $\mathbb{Z}/q\mathbb{Z}$ - module où q divise p)
- Déterminer $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ (considérer d = pgdc(m, n
(1) - Si M est simplement un A-module à gauche (A non commutatif) M^* est un A-module à dr

(3) Exemple de A-module à gauche admettant des bases de cardinaux distincts $E = \mathbb{C}[X]$
$A = \mathcal{L}(E, E)$ (applications $\mathbb{C}$-linéaires)
- Montrer que A est muni d'une structure de A-module à gauche, libre de rang 1
- Soient $\alpha, \beta \in A$ définis par

$$\alpha(P)(X^2) = \frac{P(X) + P(-X)}{2}$$

$$X \cdot \beta(P)(X^2) = \frac{P(X) - P(-X)}{2}$$

montrer que $\{\alpha, \beta\}$ est une base de A

<u>Hint</u> $P \xrightarrow{u} P(X^2)$ satisfont à : $Id = u \circ \alpha + v \circ \beta$
$P \xrightarrow{v} X P(X^2)$ $\quad \alpha \circ u = Id$, $\beta \circ u = 0$
$\alpha \circ v = 0$, $\beta \circ v = Id$

on dit que I est irréductible sinon, càd ssi $\{I = J\cap K \Rightarrow J = I$ ou $J = K\}$

× ④ Definition I ideal d'un anneau A (commutatif)
I est reductible ssi : $\exists\, J, K$ ideaux de A
$I \subsetneq J$, $I \subsetneq K$ et $I = J\cap K$

(a) $\{0\} = \bigcap\{I \mid I$ idéal irréductible de $A\}$
considérer $a \neq 0$ et $\sigma = \{I$ idéal $/ a \notin I\}$

(b) $I = \bigcap\{I' \supset I \mid I'$ irreductible $\}$

(c) déterminer les ideaux irréductibles de $\mathbb{Z}$

d) I maximal $\Rightarrow$ I premier $\Rightarrow$ I irréductible.

× ⑤ Soit A un anneau commutatif, M un a module libre muni d'une base $\{x_1, \dots, x_n\}$

a) Soit $\mathcal{P}$ un ideal maximal de A. Montrer que $M/_{\mathcal{P}.M}$ est un espace vectoriel sur $A/_{\mathcal{P}}$.

b) Montrer que les classes des x_i dans $M/_{\mathcal{P}M}$ forment une base de cet espace vectoriel. En déduire que n ne depend pas de la base choisie

<u>N.B</u> • Si I est un idéal de A, M un A module IM designe l'ensemble des sommes finies $\sum \lambda_i x_i$, $\lambda_i \in I, x_i \in M$, et dans (a) On montrera que IM est un sous A-module de M, et que $\mathcal{P}.M$ est l'ensemble des $\mu_1 x_1 + \dots + \mu_n x_n$, $\mu_i \in \mathcal{P}$, cette écriture etant unique -

• Cet exercice montre que le phenomène de l'exo ③ n'a lieu que pour des anneaux non commutatifs.

× ⑥ Soit A un anneau A^n est un A-module à gauche

• $\mathrm{Hom}_A(A^n, A) \cong A^n$

• Soit $u : M \longrightarrow N$ une application A-lineaire
${}^t u \;\; N^* \longrightarrow M^*$ ${}^t u(n^*) = n^* \circ u$

<u>Montrer</u> $*$ u surjective $\Rightarrow$ ${}^t u$ injective
et par des contre exemples :
${}^t u$ injective $\not\Rightarrow$ u surjective
u injective $\not\Rightarrow$ ${}^t u$ surjective

(4) I est réductible ssi $\exists J, K$ idéaux de A $I \subsetneq J$ et $I \subsetneq K$ et $I = J \cap K$
I irréductible sinon, càd ssi $I = J \cap K \Rightarrow J = I$ ou $J = K$.

a) $\{0\}$ = intersection des idéaux irréductibles de A.

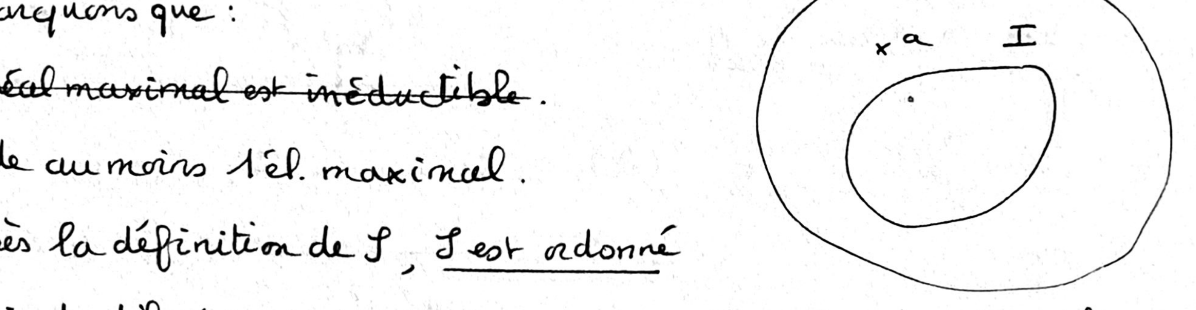
Soit $a \neq 0$, $a \in A$. Considérons $\mathcal{S} = \{ I \subset A \ / \ I$ idéal et $a \notin I \}$

Exhibons un élément irréductible dans $\mathcal{S}$.

Pour cela, remarquons que :

~~* Tout idéal maximal est irréductible~~.

* $\mathcal{S}$ possède au moins 1 él. maximal.



En effet, d'après la définition de $\mathcal{S}$, $\mathcal{S}$ est ordonné (pour l'$\subset$) et inductif (car si $(I_\lambda)_{\lambda \in \Lambda} \subset \mathcal{S}$ totalement ordonnée, alors $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ est un idéal ne contenant pas a. Donc $I \in \mathcal{S}$ et I majore la partie $(I_\lambda)_{\lambda \in \Lambda}$). Donc $\mathcal{S}$ possède au moins un élément maximal noté : I

Montrons que I, maximal dans $\mathcal{S}$, est irréductible.

Si J, K idéaux / $\begin{cases} I \subsetneq J \\ I \subsetneq K \end{cases}$ et $I = J \cap K$ alors $J \notin \mathcal{S}$ $\Rightarrow a \in J$
$\Rightarrow a \in K$

donc $a \in J \cap K = I$, ce qui est absurde.

Donc I est irréductible.

CQFD

On a montré que $\forall a \in A$ $a \neq 0$ $\exists I$ irréductible / $a \notin I$

D'où, en notant $L = \{$intersection des idéaux irréductibles de $A\}$,

on a $a \in A$ $a \neq 0 \Rightarrow a \notin L$ d'où $\complement_A \{0\} \subset \complement_A L \Leftrightarrow L \subset \{0\}$.

D'où $\boxed{L = \{0\}}$

b) $I = \bigcap \{ I' \supset I \,/\, I' \text{ irréductible} \}$ (b)

Préliminaire :

[I] Quels sont les idéaux de $A/_I$? Ce sont les $I'/_I$ où I' est un idéal de A contenant I.

$$A \xrightarrow{\varphi} A/_I \qquad \varphi = \text{homomorphisme d'anneaux.}$$

$$\mathcal{J}_A^I = \left\{ \begin{array}{c}\text{idéaux de A contenant} \\ I\end{array} \right\} \xrightarrow{\varphi} \left\{ \begin{array}{c}\text{idéaux} \\ \text{de } A/_I\end{array} \right\} = \mathcal{J}_{A/_I}$$

$$\varphi^{-1}(\mathcal{J}) \longleftarrow \mathcal{J}$$

$$I' \longrightarrow \varphi(I') = I'/_I$$

• On a $\varphi(\varphi^{-1}(\mathcal{J})) = \mathcal{J}$ ✓ car φ surjective. On a toujours $\varphi^{-1}(\varphi(I')) \supset I'$

Si $I \subset I'$, $x \in \varphi^{-1}(\varphi(I'))$ $\varphi(x) \in \varphi(I')$

$\exists y \in I'$ $\varphi(x) = \varphi(y) \Rightarrow x - y \in I \subset I'$

$\Rightarrow x \in I'$

d'où $\varphi^{-1}(\varphi(I')) = I'$.

Ainsi $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = Id$, donc φ est bijective de $\mathcal{J}_A^I$ sur $\mathcal{J}_{A/_I}$

[II] Prop. ‖ $I'/_I$ idéal irréductible de $A/_I$ $\Leftrightarrow$ I' est un idéal irréductible de A, contenant I.

On a :

$$J'/_I \cap K'/_I = \frac{J \cap K'}{I} \quad (\text{II}')$$

$I'/_I$ irréductible $\Leftrightarrow \left\{ I'/_I = J'/_I \cap K'/_I \Rightarrow I'/_I = J'/_I \text{ ou } I'/_I = K'/_I \right\}$

$\Leftrightarrow \left\{ I' = J' \cap K' \Rightarrow I' = J' \text{ ou } I' = K' \right\}$

$\Leftrightarrow$ I' irréductible.

Montrons (b)

$$\{0\} = \underbrace{\bigcap_{I' \supset I} \{ I'/_I \text{ irréductible} \}}_{\bigcap \{I' \text{ irréductibles}\}/I} \Leftrightarrow I = \bigcap \{ I' \supset I \,/\, I' \text{ irréductible} \}$$

CQFD

<u>Remarques</u> : $I \subset A$ idéal, A/I, Soit $\{J_\lambda\}_{\lambda\in\Lambda}$ une familles d'idéaux de A tels que $I \subset J_\lambda$. Considérons l'idéal $\cap\{J_\lambda/I\}_{\lambda\in\Lambda}$. On a : $\cap(J_\lambda/I)_{\lambda\in\Lambda} = \dfrac{\cap(J_\lambda)_{\lambda\in\Lambda}}{I}$

Si $x \in \bigcap_{\lambda\in\Lambda}(J_\lambda/I) \Leftrightarrow \forall\lambda\in\Lambda \; x \in J_\lambda/I \Leftrightarrow \forall\lambda\in\Lambda \; x\in J_\lambda$.

c) <u>Idéaux irréductibles de $\mathbb{Z}$</u>

Les idéaux irréductibles de $\mathbb{Z}$ sont les $n\mathbb{Z}$ qui vérifient (1)

$$n\mathbb{Z} = x\mathbb{Z} \cap y\mathbb{Z} \Rightarrow x\mathbb{Z} = n\mathbb{Z} \text{ ou } y\mathbb{Z} = n\mathbb{Z} \qquad (1)$$

Montrons que :

Pro | $n\mathbb{Z}$ irréductible $\Leftrightarrow$ $n=0$ ou $n=p^k$ où $p\in\mathcal{P}$

($\Leftarrow$) • Si $n=0$, $0\mathbb{Z} = J\cap K = x\mathbb{Z}\cap y\mathbb{Z} \Rightarrow xy \in 0\mathbb{Z} \Rightarrow xy=0$
d'où $x=0$ ou $y=0$

• Si $n=p^k$ où $k\in\mathbb{N}$ et $p\in\mathcal{P}$ ($p>0$), considérons
$p^k\mathbb{Z} = x\mathbb{Z}\cap y\mathbb{Z}$

$\begin{cases} x\mid p^k \Rightarrow \exists\alpha\in\mathbb{N} \,/\, x=p^\alpha \\ y\mid p^k \Rightarrow \exists\beta\in\mathbb{N} \,/\, y=p^\beta \end{cases}$ d'où $p^k\mathbb{Z} = p^\alpha\mathbb{Z}\cap p^\beta\mathbb{Z}$

Comme $p^{\alpha}\mathbb{Z} \cap p^{\beta}\mathbb{Z} = \mu(p^{\alpha}, p^{\beta})\mathbb{Z} = p^{\operatorname{Sup}(\alpha,\beta)}\mathbb{Z}$, on en déduit que $x = p^k$ ou $y = p^k$.

($\Rightarrow$) Inversement, soit $n\mathbb{Z}$ irréductible et tel que $n \neq 0$. Ou bien $n = 1$, et c'est terminé. Ou bien $n \neq 1$. Alors n possède au moins 1 ~~facteur~~ diviseur p premier. Montrons que $n = p^k$ où $k \in \mathbb{N}$.

$n = p^k q$ où $\Delta(p, q) = 1$, et donc $\mu(p^k, q) = n$

D'où : $n\mathbb{Z} = p^k\mathbb{Z} \cap q\mathbb{Z} \Rightarrow n = p^k$ ou $n = q$

$n \neq q$ car autrement $n = p^k . n \Rightarrow p^k = 1 \Rightarrow k = 0$, absurde car $p | n$.

Donc $n = p^k$.

CQFD

(Remarque : d'habitude, on exclus l'anneau A pour l'irréductibilité)

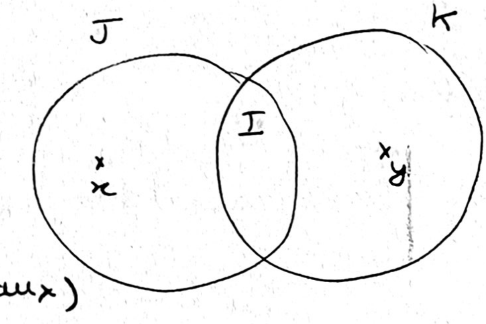
d) | I maximal $\Rightarrow$ I premier |

fait sur le Querré, Th 1. p 59.

| I premier $\Rightarrow$ I irréductible |

Par l'absurde, si I premier et I réductible,

alors $\exists J, K \;/\; I = J \cap K$ et $I \subsetneq J$ et $I \subsetneq K$.



Soit $x \in J \setminus I$ et $y \in K \setminus I$.

On a $xy \in J \cap K$ (car I et K sont des idéaux)

Donc $xy \in I \Rightarrow x \in I$ ou $y \in I$, ce qui est absurde.

Remarque : $IJ = \{ \sum_{i=1}^{n} x_i y_i \,/\, x_i \in I \text{ et } y_i \in J,\ n \in \mathbb{N} \}$

(Exo)

1) IJ est un idéal de A, c'est l'idéal engendré par $\{ xy \,/\, x \in I \text{ et } y \in J \}$

2) $IJ \subset I \cap J$. Montrer qu'on peut avoir $IJ \subsetneq I \cap J$

3) Si $\mathcal{P}$ est un idéal premier, $I \cap J \subset \mathcal{P} \Rightarrow I \subset \mathcal{P}$ ou $J \subset \mathcal{P}$.

4) $\mathcal{P} \subset \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_n$ avec $\mathcal{P}_i$ premiers $\Rightarrow \exists i \,/\, \mathcal{P} \subset \mathcal{P}_i$

---

2) $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$ puisque $\forall x \in (m\mathbb{Z})(n\mathbb{Z})$

$x = \sum m x_i \, n y_i \in mn\mathbb{Z}$

D'où $(m\mathbb{Z})(n\mathbb{Z}) \subset mn\mathbb{Z}$ et $(m\mathbb{Z})(n\mathbb{Z})$ contient mn, d'où $=$.

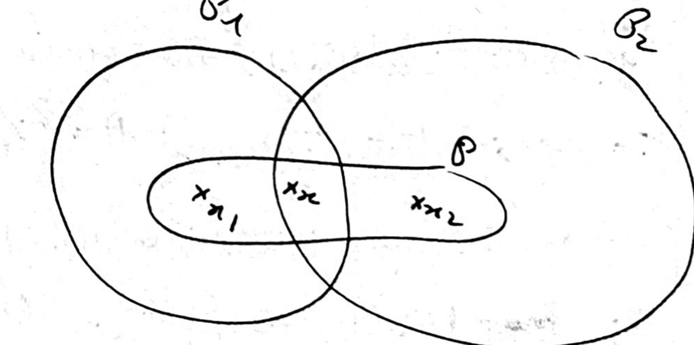
De plus $(m\mathbb{Z})(n\mathbb{Z}) \subset m\mathbb{Z} \cap n\mathbb{Z}$ si $\Delta(m,n) \neq 1$.

4)

$n=2$

Supposons, par l'absurde, que $\begin{cases} \mathcal{P} \not\subset \mathcal{P}_1 \Rightarrow \exists x_2 \in \mathcal{P} \setminus \mathcal{P}_1 & x_2 \in \mathcal{P}_2 \\ \mathcal{P} \not\subset \mathcal{P}_2 \Rightarrow \exists x_1 \in \mathcal{P} \setminus \mathcal{P}_2 & x_1 \in \mathcal{P}_1 \end{cases}$

$x = x_1 + x_2 \in \mathcal{P} \subset \mathcal{P}_1 \cup \mathcal{P}_2$



$\begin{cases} \text{si } x \in \mathcal{P}_1, \text{ on a } x_2 \in \mathcal{P}_1 \text{ absurde} \\ \text{si } x \in \mathcal{P}_2, \text{ on a } x_1 \in \mathcal{P}_2 \text{ absurde} \end{cases}$

NB : on n'a pas utilisé le fait que $\mathcal{P}_1$ et $\mathcal{P}_2$ étaient premiers :

Pro $\|$ $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}$ 3 idéaux (qcq) $\mathcal{P} \subset \mathcal{P}_1 \cup \mathcal{P}_2 \Rightarrow \mathcal{P} \subset \mathcal{P}_1$ ou $\mathcal{P} \subset \mathcal{P}_2$.

n quelconque : récurrence. Le théorème est vrai pour $n-1$ idéaux premiers. $(n \geq 2)$

* Si $\mathcal{P} \subset \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \ldots \cup \mathcal{P}_n$, on aurait $\mathcal{P} \subset \mathcal{P}_k$ (hyp. réc.)
* Si l'on a $\mathcal{P} \not\subset \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \ldots \cup \mathcal{P}_n$ $\forall i \in [1,n]$,

on a :

Il existe $y_i \in \mathcal{P}$ et $y_i \not\in \mathcal{P}_1 \cup \ldots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \ldots \cup \mathcal{P}_n \Rightarrow y_i \in \mathcal{P}_i$

donc $y_i \in \mathcal{P}_i$ et $y_i \notin \mathcal{P}_j$ pour $j \neq i$. (où $y_i \in \mathcal{P}$)

Si $\forall i$ $x_i \notin \mathcal{P}_i$ $\forall j \neq i$ $x_j \in \mathcal{P}_i$ $\quad x_1 + \dots + x_i + \dots + x_n \notin \mathcal{P}_i$ (avec $x_i \notin \mathcal{P}_i$)

On prend $x_i = y_1 \cdots y_{i-1} y_{i+1} \cdots y_n \in \mathcal{P}_j$ $\forall j \neq i$

$\notin \mathcal{P}_i$ car $\mathcal{P}_i$ premier

$(x_i \in \mathcal{P}_i \Rightarrow \exists k \neq i \; y_k \in \mathcal{P}_i$ absurde)

Ainsi $x_i \in \mathcal{P}$ $\forall i$ et $x_1 + \dots + x_n \notin \mathcal{P}_1 \cup \dots \cup \mathcal{P}_n$.

C'est absurde.

Dans tous les cas ~~$\mathcal{P} \subset$~~ $\exists i \; / \; \mathcal{P} \subset \mathcal{P}_1 \cup \dots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_i \cup \dots \cup \mathcal{P}_n$

CQFD

(Exo)

Soit A un anneau commutatif unitaire

$$\mathrm{Nil}(A) = \{x \in A \; / \; \exists n \in \mathbb{N} \; x^n = 0\}$$

C'est le nilradical de l'anneau A.

1°/ Déterminer $\mathrm{Nil}(A)$ dans chacun des cas : $A = K[X]/(X^n)$ où K = corps ; $A = \mathbb{Z}/p^k\mathbb{Z}$; $A = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \dots \times p_s^{k_s}\mathbb{Z}$

2°/ Montrer que $\mathrm{Nil}(A)$ est un idéal de A.

3°/ ~~Band~~ $\mathrm{Nil}(A) = \bigcap_{\mathcal{P} \text{ idéal premier}} \mathcal{P}$. (cf. Queré)

1°/ $A = \mathbb{Z}/p^k\mathbb{Z}$ $\quad \dot{x} \in \mathrm{Nil}(A) \Leftrightarrow \exists n \in \mathbb{N} \; / \; p^k \mid x^n$

$\Leftrightarrow p \mid x$

$\Leftrightarrow \exists \lambda \in \mathbb{Z} \; / \; \dot{x} = \lambda \dot{p} = \dot{p}\dot{\lambda}$

$$\mathrm{Nil}(\mathbb{Z}/p^k\mathbb{Z}) = p \, \mathbb{Z}/p^k\mathbb{Z}$$

On montre, de même, que $\mathrm{Nil}\, A = X \, K[X]/(X^n)$

mardi
15 janvier 80 : Théorème Chinois.

a_i idéal de A. Je dis que a_1 et a_2 sont étrangers (premiers entre eux) si $a_1 + a_2 = A$.

(On suppose A anneau commutatif et unitaire)

1) Montrer que $a_1 + a_2 = A \Longrightarrow a_1 . a_2 = a_1 \cap a_2$. Envisager la réciproque.

2) Montrer que $A/a_1 \times A/a_2 \simeq A/a_1 \cap a_2$ (si $a_1 + a_2 = A$)

3) généralisation : $a_1, \dots, a_n$ deux à deux étrangers. Montrer qu'alors

α) $a_1 + a_2 \dots a_n = A$ et $a_1 \dots a_n = a_1 \cap \dots \cap a_n$

β) $A/a_1 \cap \dots \cap a_n \simeq A/a_1 \times \dots \times A/a_n$

γ) $A/a_1 \cap \dots \cap a_n \longrightarrow A/a_1 \times \dots \times A/a_n$

$x \longmapsto (x, \dots, x)$ est un isomorphisme de groupes.

---

1) Si $a_1 + a_2 = A$, montrons que $a_1 \cap a_2 \subset a_1 . a_2$.

$\forall x \in a_1 \cap a_2 \quad 1 = x_1 + x_2 \quad x_1 \in a_1 \quad x_2 \in a_2$

d'où $x = \underbrace{x x_1}_{\in a_1 a_2} + \underbrace{x x_2}_{\in a_1 a_2} \in a_1 . a_2$.

Exemple : $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z} \Longleftrightarrow n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z} = (n\mathbb{Z}).(m\mathbb{Z})$

On a l'équivalence dans n'importe quel anneau principal, et en particulier dans $K[X]$ où K est un corps.

⚠ Il existe des anneaux A tels que $a_1 . a_2 = a_1 \cap a_2$ et pourtant $a_1 + a_2 \neq a$.

Prenons $A = K[X, Y]$, $a_1 = (X)$ et $a_2 = (Y)$.

$$\begin{cases} a_1 \cap a_2 = (XY) & \text{car } a_1 = \{P \,/\, P(0,Y) = 0\} \, ; \, a_2 = \{Q \,/\, Q(X,0) = 0\} \\ a_1 a_2 = (XY) \end{cases}$$

donc $a_1 a_2 = a_1 \cap a_2$

Et pourtant $\mathfrak{a}_1 + \mathfrak{a}_2 = \{ PX + QY \,/\, P, Q \in K[X,Y] \} \neq \mathfrak{a}$ car

$1 \notin \mathfrak{a}_1 + \mathfrak{a}_2$ (cf. $PX + QY = 1 \Rightarrow 0 = 1$ absurde).

[NB : autre façon de conclure : $\mathfrak{a}_1 + \mathfrak{a}_2 = \{ P \,/\, P(0,0) = 0 \} \Rightarrow 1 \notin \mathfrak{a}_1 + \mathfrak{a}_2$]

2)

La suite : $0 \longrightarrow \mathfrak{a}_1 \cap \mathfrak{a}_2 \xrightarrow{i} A \xrightarrow{f} A/\mathfrak{a}_1 \times A/\mathfrak{a}_2$ est exacte (de groupes +)

$x \longmapsto (\dot{x}, \bar{x})$

Tout le problème consiste à montrer que f est surjective.

Je pose $1 = x_1 + x_2$.

Résolvons $\begin{cases} y = y_1 \mod \mathfrak{a}_1 \\ y = y_2 \mod \mathfrak{a}_2 \end{cases}$ (1)

On a : $(\dot{x}_2, \bar{x}_2) = (\dot{1}, \bar{0})$

$(\dot{x}_1, \bar{x}_1) = (\dot{0}, \bar{1})$

On prend ~~$y = y_1(\dot{1},\bar{0}) + y_2(\dot{0},\bar{1})$~~

$y = y_1 x_2 + y_2 x_1$. On a bien $(\dot{y}, \bar{y}) = (\dot{y}_1, \bar{y}_2)$.

ce qui donne 1 solution de (1).

$\forall y'$ solution, $y - y' \in \mathfrak{a}_1 \cap \mathfrak{a}_2$

<u>Application</u> : Dans $\mathbb{Z}$ $\begin{cases} y \equiv y_1 & [a_1] \\ y \equiv y_2 & [a_2] \end{cases}$ où $\Delta(a_1, a_2) = 1$

admet 1 solution et 1 seule modulo le ppcm (a_1, a_2).

C'est la classe de $y_1 a_1 v + y_2 a_1 u$ où $a_1 u + a_2 v = 1$

3) α) Pour n idéaux $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ tels que $\mathfrak{a}_i + \mathfrak{a}_j = A \quad \forall i \neq j$.

$\begin{cases} 1 = x_{12} + x_2 \\ 1 = x_{13} + x_3 \\ \vdots \\ 1 = x_{1n} + x_n \end{cases}$

$1 = \prod_{j=2}^{n} (x_{1j} + x_j)$

$1 = \underbrace{x'_1}_{\in \mathfrak{a}_1} + x_2 \ldots x_n \in \mathfrak{a}_1 + \mathfrak{a}_2 \ldots \mathfrak{a}_n$

On montre que $a_1 \dots a_n = a_1 \cap \dots \cap a_n$ par récurrence sur n.
C'est vrai pour $n=2$. Vrai au rang $n-1$:

$$a_1 a_2 \dots a_n = a_1 \cdot (a_2 \dots a_n) = a_1 \cdot \cap a_2 \dots a_n = a_1 \cap a_2 \cap \dots \cap a_n$$

CQFD

β) Montrons que $A/_{a_1 \cap \dots \cap a_n} \simeq A/_{a_1} \times \dots \times A/_{a_n}$

$$\dot{x} \xrightarrow{\beta} (\dot{x}_{(1)}, \dots, \dot{x}_{(n)})$$

Résolvons
$$\begin{cases} y \equiv y_1 & \text{mod } a_1 \\ \dots \\ y \equiv y_n & \text{mod } a_n \end{cases}$$

- on note $1 = x_1 + x_2 \dots x_n$ (cf. α))

Notons $z_1 = x_2 \dots x_n$, alors $\beta(z_1) = (\dot{1}_{(1)}, \dot{0}_{(2)}, \dots, \dot{0}_{(n)})$

De la même façon, $1 = x_i + x_1 \dots x_{i-1} x_{i+1} \dots x_n$, on pose $z_i = 1 - x_i$.
Alors : $\beta(z_i) = (\dot{0}_{(1)}, \dots, \dot{1}_{(i)}, \dots, \dot{0}_{(n)})$

Une des solutions est $y = \sum_{i=1}^{n} y_i z_i$. La solution est unique modulo $a_1 \cap \dots \cap a_n$.

- γ) c'est le β.

Application numérique :

Trouver x positif minimum
$$\begin{cases} x \equiv 4 & \text{mod}(11) \\ x \equiv 3 & \text{mod}(9) \\ x \equiv 2 & \text{mod}(5) \end{cases}$$

Il existe 1 solution unique modulo $11 \times 9 \times 5 = 495$.

$\pi(n_1) = (1,0,0)$ $\quad n_1 = 45 \equiv 1 [11]$ $\quad$ On prend $x = 45 \times 4 + 55 \times 3 + 297$
$\pi(n_2) = (0,1,0)$ $\quad n_2 = 55$ $\quad x = 642$
$\pi(n_3) = (0,0,1)$ $\quad \underbrace{99}_{11 \times 9} \equiv 4 [5] \Rightarrow \underbrace{3 \times 99}_{297} \equiv 2 [5]$

$x = 642 + \lambda \, ppcm(11, 9, 5) \quad \lambda \in \mathbb{Z}$

le plus petit x positif est $x = 642 - 495 = 147$

Exercice

Soient :

$r(A) = \bigcap \{ \mathfrak{M} \in A \,/\, \mathfrak{M} \text{ idéal maximal} \}$ = radical de A

$A^* = \{ x \in A \,/\, \exists y \in A \quad xy = 1 \}$ est un groupe pour $\times$.

$(\mathbb{Z}^* = \{\pm 1\} \;; (\mathbb{R}[X])^* = \mathbb{R}^*)$

Montrer que $x \in r(A) \Leftrightarrow \forall y \in A \quad 1 - xy \in A^*$

Solution :

$(\Leftarrow)$

$x \notin r(A) \Leftrightarrow \exists \mathfrak{M}$ idéal maximal $/ \, x \notin \mathfrak{M}$

$\Leftrightarrow \quad xy = 1 + m$ où $m \in \mathfrak{M}$

$\Leftrightarrow \quad 1 - xy \in \mathfrak{M}$ maximal $\Rightarrow 1 - xy \notin A^*$ (sinon $\mathfrak{M} = A$)

$(\Rightarrow)$ Supposons que $x \in r(A)$ et que $1 - xy \notin A^*$.

Alors $\exists \mathfrak{M}$ idéal maximal contenant $1 - xy$.

$$\left. \begin{array}{r} 1 - xy \in \mathfrak{M} \\ \text{et } x \in \mathfrak{M} \end{array} \right\} \Rightarrow 1 \in \mathfrak{M} \Rightarrow \mathfrak{M} = A, \text{ absurde}.$$

Donc $1 - xy \in A^*$.

<u>Remarque</u> : $r(\mathbb{Z}) = \{0\}$ car $r(\mathbb{Z}) = \bigcap_{p \in \mathcal{P}} p\mathbb{Z}$ et $\mathcal{P}$ est infini.

Essayons de trouver un exemple de $r(A)$ non banal. Pour cela, considérons le corps des fractions rationnelles $K(X) = \{ \frac{P}{Q} \,/\, P, Q \in K[X] \}$

Soit $K(X)_0 = \{ P/Q \in K[X] \,/\, Q(0) \neq 0 \} = A$

On a $P(0) \neq 0 \iff P/_Q$ inversible dans $K(X)_0$

Soit $\mathcal{M} = \{ P/_Q \in A \ / \ P(0) = 0 \}$. C'est un idéal ~~de~~ maximal (car si $\frac{P'}{Q'} \notin \mathcal{M}$, $\mathcal{M} + \left(\frac{P'}{Q'}\right) = K(X)_0$ car $P'(0) \neq 0 \Rightarrow \frac{P'}{Q'}$ inversible dans $K(X)_0$

Il est clair (ou obscur) que $r(A) = \mathcal{M}$.

En effet, tout idéal différent de A est dans $\mathcal{M}$ (sinon ...).

généralisation :

lundi 21 janvier

Théorème : Soit A un anneau. Les 2 conditions suivantes sont équivalentes :

1) $A \setminus A^*$ est un idéal

2) A possède un seul idéal maximal

Définition : Un tel anneau est dit "anneau local".

(exo : l'anneau des séries entières convergentes est un anneau local)

2) ⇒ 1) $\mathfrak{M}$ est l'idéal maximal de A.

$\forall x \notin \mathfrak{M}$ on a $xA \neq A$. On, il existe un idéal maximal qui contient xA. Ce ne peut être que $\mathfrak{M}$: $xA \subset \mathfrak{M} \iff x \notin A^*$

D'où $\mathfrak{M} = A \setminus A^*$

1) ⇒ 2) Si I est un idéal propre de A, $I \subset A \setminus A^*$. ~~Si~~ Donc si $A \setminus A^*$ est un idéal, c'est forcément ~~un~~ l'idéal maximal de A.

[cf : Soit J un idéal maximal quelconque, $J \subset A \setminus A^* \Rightarrow J = A \setminus A^*$]

CQFD

Exercice : Montrer que l'anneau $\mathbb{Z}/_{p^n\mathbb{Z}}$ est local.

Solution : $A = \mathbb{Z}/_{p^n\mathbb{Z}}$ $\dot{k} \in \mathbb{Z}/_{p^n\mathbb{Z}}$. Cherchons A^*.

$$A^* = \{ \dot{k}' \in A \ / \ \Delta(k', p^n) = 1 \}$$

Ici $\dot{k} \in A^* \iff p \nmid k$ donc $A \setminus A^* = p\left(\mathbb{Z}/_{p^n\mathbb{Z}}\right)$ est un idéal

(NB : m̂ chose avec $K[X]/_{(X^n)}$)

Exercice : $K[[X]]$, anneau des séries formelles, est un anneau local dont l'idéal maximal est $XK[[X]]$

Solution : $A \setminus A^* = XK[[X]]$ est un idéal.

cf : $P \in A^* \Leftrightarrow P(0) \neq 0$.

Anneaux des fractions : Soit A un anneau,

S est une partie multiplicative si $x, y \in S \Rightarrow xy \in S$. Supposons que $0 \notin S$ et considérons $A \times S$ muni de la relation d'équivalence suivante :

$$(x, s) \sim (x', s') \Leftrightarrow s''xs' = x'ss'' \ \exists s'' \in S$$
$$\Leftrightarrow s''(xs' - x's) = 0 \quad s'' \in S.$$

(NB : Si A est intègre, on pourra supprimer s'')

Alors $A_S = A \times S / \sim$ est un anneau.

En notant $\widehat{(x, s)} = \frac{x}{s}$, on pose $\varphi : A \longrightarrow A_S$
$x \longmapsto \frac{x}{1}$ (~~...~~)

(NB : si $1 \notin S$, $\frac{sx}{s} = \frac{x}{1}$ bien connu)

φ est un homomorphisme, $\varphi(A) \subset A_S^*$ et φ est injective dès que A est intègre

(Note sur s'' : si $sx = 0 \Rightarrow \varphi(s)\varphi(x) = 0$. On veut que $\varphi(s)$ soit inversible, et donc que $\varphi(x) = 0 \Rightarrow \frac{x}{1} = \frac{0}{1} \Leftrightarrow x.1 = 0.1 \Leftrightarrow x = 0$. Ainsi, on veut que ~~...~~ $\varphi(s)\varphi(x) = 0 \Rightarrow x = 0$.)

Solution :

* $\sim$ est d'équivalence : RST

Si $(x_1, s_1) \sim (x_2, s_2) \Leftrightarrow s'(x_1 s_2 - s_1 x_2) = 0 \Rightarrow s'' s_3 s'(x_1 s_2 - s_1 x_2) = 0$

$(x_2, s_2) \sim (x_3, s_3) \Leftrightarrow s''(x_2 s_3 - s_2 x_3) = 0 \Rightarrow s' s_1 s''(x_2 s_3 - s_2 x_3) = 0$

$$s's''(x_1 s_2 s_3 - s_1 s_2 x_3) = 0$$
$$s's'' s_2 (x_1 s_3 - s_1 x_3) = 0$$
$$\Downarrow$$
$$(x_1, s_1) \sim (x_3, s_3) \quad \text{oui.}$$

(NB : Si l'on n'avait pas s'', on n'aurait pas pu conclure)

(NB : Si A était intègre, on aurait raisonné différemment)

* A_S est un anneau : On pose :

$$\dot{\overline{(x,s)}} + \dot{\overline{(x',s')}} = \dot{\overline{(xs'+x's, ss')}}$$

et

$$\dot{\overline{(x,s)}}\,\dot{\overline{(x',s')}} = \dot{\overline{(xx', ss')}}$$

Ces opérations sont bien définies : Prenons $\dot{\overline{(x,s)}} = \dot{\overline{(x_1,s_1)}}$, c-à-d $\exists s'' \mid s''(x s_1 - x_1 s) = 0$

Alors a-t-on $\dot{\overline{(xs'+x's, ss')}} = \dot{\overline{(x_1 s' + x' s_1, s_1 s')}}$?

oui, puisque $s_1 s'(xs'+x's) - ss'(x_1 s' + x' s_1) = s'^2 (s_1 x - s x_1) = \alpha$

d'où : $s''\alpha = s'^2 s''(s_1 x - s x_1) = 0$.

On fait de m̂ pour la loi ×.

On vérifie, comme pour $\mathbb{Q}$, que $(A_S, +, .)$ est un anneau, unitaire d'élément unité $\frac{s}{s}$ ($\frac{1}{1}$ si $1 \in S$), puisque

$$\dot{\overline{(s,s)}}\,\dot{\overline{(x',s')}} = \dot{\overline{(sx', ss')}} = \dot{\overline{(x',s')}}$$

* φ est un morphisme : oui, et $[\varphi(s)]^{-1} = \left[\frac{s}{1}\right]^{-1} = \frac{1}{s} \Rightarrow \varphi(A) \subset A_S^*$

* $\mathrm{Ker}\,\varphi$? $\mathrm{Ker}\,\varphi = \{x \mid \exists s'' \in S \ \ x s'' = 0\} \subset A$ (est un idéal de A)

Il est clair que $\mathrm{Ker}\,\varphi = \{0\}$ si A est intègre, et même si S ne contient pas de diviseurs de 0.

CQFD

Exemples : ① Si A est intègre, on prend $S = A \setminus \{0\} = A^*$ et on construit le corps des fractions de A : $K = A_S$ est un corps..

$$\varphi : A \hookrightarrow K \quad \text{homomorphisme inj. d'anneaux,}$$

L'existence d'un plongement (φ monomorphisme ~~inj~~ d'anneaux) de A dans un corps K équivaut au fait que A soit intègre.

② Si A non intègre, on peut toujours prendre $S = A^*$, ou S = {ensemble des non diviseurs de 0} (qui est une partie multiplicative :

$s, s' \in S \quad ss'x = 0 \Rightarrow s'x = 0 \Rightarrow x = 0$.)

Dans ce cas φ est injective, et A_S est alors appelé "anneau total des fractions de A".

L'exemple ② est bien moins utilisable que ①.

③ Soit $\mathbb{Z}$ et $\mathbb{Q}$. Posons $S = \mathbb{Z} \setminus p\mathbb{Z}$. S est multiplicatif dès que p est premier, car $x, y \in S \Rightarrow xy \in S$ ($p \nmid x$ et $p \nmid y \Rightarrow p \nmid xy$)

$\mathbb{Z}_S = \{ \frac{m}{n} \ / \ p \nmid n$ (p premier)$\}$ est considérée comme partie de $\mathbb{Q}$.

D'où l'exercice :

<u>Exercices:</u> 1) A intègre, pour toute partie multiplicative S, on a des injections $A \overset{\varphi}{\hookrightarrow} A_S \hookrightarrow K$ et $A_S = \{ \frac{x}{y} \in K \ / \ y \in S \}$ (après identification)

Par exemple $K(X)_0 = \{ \frac{P}{Q} \ / \ Q(0) \neq 0 \}$ (ici $S = \{ Q \ / \ Q(0) \neq 0 \}$)

2) Si $\mathcal{P}$ est un idéal premier, a) montrer que $S = A \setminus \mathcal{P}$ est une partie multiplicative. Dans ce cas là, on note $A_{\mathcal{P}} = A_S$. b) Montrer que $A_{\mathcal{P}}$ est un anneau local dont l'idéal maximal est $\mathcal{P} A_{\mathcal{P}} = \{ \frac{x}{s} \ / x \in \mathcal{P}$ et $s \notin \mathcal{P} \}$

dimanche 27 (Sup.) TD5

Note : ~~Si A = A-module à gauche,~~ alors M (M A)

(6) A anneau com. unit. A^n est un A-module.

* $\mathrm{Hom}_A(A^n, A) \simeq A^n$

Soit $f \in \mathrm{Hom}_A(A^n, A)$. $\forall x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in A^n$ $\quad f(x) = \sum_{i=1}^{n} x_i f(e_i)$ où $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ i-pl

Considérons

$$\varphi : \mathrm{Hom}_A(A^n, A) \longrightarrow A^n$$
$$f \longmapsto \begin{pmatrix} f(e_1) \\ \vdots \\ f(e_n) \end{pmatrix}$$

φ est bijective, et c'est un homomorphisme ~~d'anneaux~~ de A-modules, puisque

$$\begin{cases} \varphi(f+g) = \varphi(f) + \varphi(g) \\ \varphi(\lambda f) = \begin{pmatrix} \lambda f(e_1) \\ \vdots \\ \lambda f(e_n) \end{pmatrix} = \lambda \varphi(f) \quad \forall \lambda \in A \end{cases}$$

* $M \xrightarrow{u} N$

$M^* \xleftarrow{{}^t u} N^*$ $\quad$ $\boxed{{}^t u(n^*) = n^* \circ u}$

(càd : on définit ${}^t u$ par dualité, en posant $\langle {}^t u(n^*), m \rangle = \langle n^*, u(m) \rangle$)

<u>Alors u surjective $\Rightarrow$ ${}^t u$ injective</u>

C'est simple. Il suffit d'écrire que ${}^t u(n^*) = {}^t u(k^*) \Leftrightarrow n^* \circ u = k^* \circ u$

càd $n^*(u(m)) = k^*(u(m)) \quad \forall m \in M$.

Si u est surjective, $\forall n \in N \quad \exists m \in M \,/\, u(m) = n$, et par suite

$$n^*(n) = k^*(n) \quad \forall n \in N$$

d'où $n^* = k^*$

cqfd

Remarque : M^* est toujours un A-module à droite si M est un A-module à gauche, grâce à la multiplication : $M^* \times A \to M^*$
$m^*, a \mapsto m^*.a$ / $m^*.a(x) = m^*(x) \times a$

Alors ${}^t u$ est A-linéaire et il suffit de parler de Noyau.

Contre-exemples :

α) ${}^t u$ injective $\not\Rightarrow$ u surjective

VOIR (*) ci-derrière.

~~$M \xrightarrow{u} N$~~

~~${}^t u$ injectif $\Leftrightarrow \{ {}^t u(\varphi) = 0 \Rightarrow \varphi = 0 \} \Leftrightarrow \{ \varphi \circ u = 0 \Rightarrow \varphi = 0 \}$~~

~~et u non surjectif.~~

~~Prenons $0 \xrightarrow{u} N \xrightarrow{\varphi} A$ où u non surjectif, et $\varphi \circ u = 0$ et φ~~ cf (*) $\rightarrow$

β) u injective $\not\Rightarrow$ ${}^t u$ surjective

$M \subset N$ $\quad {}^t u : M \longrightarrow N$
$m \longmapsto u(m) = m$ est injective.

Et pourtant, $M = 2\mathbb{Z} \subset N = \mathbb{Z}$

$\varphi : 2\mathbb{Z} \longrightarrow \mathbb{Z}$
$2k \longmapsto k$ est injective, et $\varphi \notin \mathrm{Im}({}^t u)$: En effet :
sinon $\varphi(2) = 1$ et $\varphi(2) = 2\varphi(1) \Rightarrow 1 =$ paire ou nul
absurde.
donc φ ne s'étend pas à $\mathbb{Z}$.

NB $\varphi \in \mathrm{Im}\,{}^t u \Leftrightarrow \exists\, n^* \in \mathbb{Z}^* / \quad \varphi(n^*) = n^*$

(*) Exemple : $\{0\} \xrightarrow[\text{injectif}]{u} \mathbb{Z}/n\mathbb{Z}$ $\quad n \geq 2$ (comme $\mathbb{Z}$-modules)

On a bien $\begin{cases} {}^t u : (\mathbb{Z}/n\mathbb{Z})^* \to \{0\}^* \text{ est injectif car } \mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^* \\ u \text{ non surjectif.} \end{cases}$

$\mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Card}\,\{\underbrace{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})}_{=\{0\}}\} = 1$

4/2/80

Exercice : A anneau unitaire
B ensemble

Trouver un A-module à gauche M tel que :

1) Il existe une injection $B \xhookrightarrow{i} M$

2) Pour toute application $B \xrightarrow{\varphi} N$ module à gauche, il existe un homomorphisme $\bar{\varphi} : M \xrightarrow{\bar{\varphi}} N$ tel que $\bar{\varphi} \circ i = \varphi$, unique.

$$\begin{array}{ccc} M & \xrightarrow{\bar{\varphi}} & N \\ i \uparrow & \nearrow \varphi & \\ B & & \end{array}$$

a) 2 solutions M_1 et M_2 sont isomorphes.

b) Il existe une solution M.

- Solution : a) On a

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ i_1 \uparrow & \nearrow i_2 & \\ B & & \end{array} \qquad f \circ i_1 = i_2$$

De même, on a l'existence de $g : M_2 \to M_1$ / $g \circ i_2 = i_1$

donc $g \circ f \circ i_1 = i_1$ où $g \circ f : M_1 \to M_1$.

$$\begin{array}{ccc} M_1 & \xrightarrow[Id]{g \circ f} & M_1 \\ i_1 \uparrow & \nearrow i_1 & \\ B & & \end{array}$$

le 2) montre l'unicité de $\bar{\varphi}$, donc ici : $g \circ f = Id$. De m̂ : $f \circ g = Id$, donc

- M_1 et M_2 sont isomorphes.

b) $A^B = \{ (a_i)_{i \in B} /$ applications $B \to A \}$ est un module à gauche sur A.

Posons $A^{(B)} = \{ (a_i)_{i \in B} \;/\; \# \{ i \;/\; a_i \neq 0 \} < \infty \} \subset A^B$ est un sous-module à gauche de A^B.

(Note : Si B est fini $A^B = A^{(B)}$)

Montrons que $A^{(B)}$ vérifie 1) et 2), et donc que $A^{(B)}$ est solution :

- Pour le 1) : Soit $i : B \longrightarrow A^{(B)}$

$$b \longmapsto i(b) = (a_{b'})_{b' \in B} \;/\; \begin{cases} a_{b'} = 0 \text{ si } b' \neq b \\ a_b = 1 \end{cases}$$

i est injective.

<u>Note</u> : $(a_b)_{b\in B} = \sum_{b\in B} a_b e_b$ où $e_b = i(b) \in A^{(B)}$
(Somme finie)

Tous les éléments de $A^{(B)}$ s'écrivent sous cette forme et de manière unique.
On dit que $(e_b)_{b\in B}$ est une base du A-module $A^{(B)}$.

• <u>Pour 2)</u> : Soit $\varphi : B \to N$
$b \mapsto \varphi(b)$

$$\begin{array}{ccc} A^{(B)} & \overset{\bar\varphi}{\dashrightarrow} & N \\ i \uparrow & \nearrow_{\varphi} & \\ B & & \end{array}$$

Si $\bar\varphi$ existe,
Nécessairement, $\bar\varphi \circ i(b) = \varphi(b) \Leftrightarrow \bar\varphi(e_b) = \varphi(b)$
Donc, nécessairement, $\underbrace{\bar\varphi\left(\sum_{b\in B} a_b e_b\right) = \sum_{b\in B} a_b \varphi(b)}$

(les sommes qui interviennent sont finies, et ont donc un sens dans les A-modules $A^{(B)}$ et N)

Donc $\bar\varphi$ est unique.

Montrons que $\bar\varphi$ ainsi défini convient : on a $\begin{cases} (1) & \bar\varphi(e_b) = \varphi(b) \\ (2) & \bar\varphi((a_b)_{b\in B}) = \sum_{b\in B} a_b \varphi(b) \end{cases}$

c.à.d que $\bar\varphi$ est bien un homomorphisme de A-modules à gauche.

$$\begin{cases} \bar\varphi((a a_b)_{b\in B}) = \sum_{b\in B} a a_b \varphi(b) = a \bar\varphi((a_b)_{b\in B}) \\ \bar\varphi((a_b + c_b)_{b\in B}) = \bar\varphi((a_b)_{b\in B}) + \bar\varphi((c_b))_{b\in B} \end{cases}$$

CQFD

<u>Définition</u> : $A^{(B)}$ est le A-module libre à gauche construit sur B.

<u>Remarque</u> : * On peut supprimer que l'hypothèse i injectif.
* On n'a pas eu besoin de la propriété $1.x = x$

exercice (5)

M = module libre de type fini de base $\{x_1, \dots, x_n\}$ sur A commutatif.

1) I idéal $IM = \left\{ \sum_{i=1}^{p} a_i m_i \;/\; a_i \in I \;\; m_i \in M \right\}$ = sous-module de M.

Montrer que $M/_{IM}$ est un $A/_I$-module.

On sait (cf. cours) que $M/_{\text{sous-module de } M}$ = A-module.

Définissons $\dot{k}\dot{m} = \dot{\overline{km}}$ où $k \in A/_I$ et $\dot{m} \in M/_{IM}$. On le peut. En effet, si $\begin{cases} \dot{k} = \dot{k}' \iff k - k' \in I \\ \dot{m} = \dot{m}' \iff m - m' = \sum_{i=1}^{p} a_i m_i \quad \in IM \end{cases}$

Alors $km - k'm' = km + k'\left(\sum_{i=1}^{p} a_i m_i - m\right)$

$km - k'm' = \underbrace{(k - k')}_{\in I} m + k' \sum_{i=1}^{p} a_i m_i \in IM$

d'où :

> **Proposition** : M module sur A, commutatif. I idéal de A.
>
> IM est un sous-module de M
>
> et $M/_{IM}$ est un $A/_I$-module

NB : $IM = \left\{ \sum_{i=1}^{p} a_i m_i \;/\; a_i \in I \;\; m_i \in M \right\}$

> **Proposition** :
> Supposons M libre. Alors $M/_{IM}$ est un module libre de type fini de base $(\dot{x}_1, \dots, \dot{x}_n)$ sur $A/_{IM}$

(R) $m \in IM$ $\exists ! \lambda_k \in I$ $/ \; m = \sum_{k=1}^{n} \lambda_k x_k$. En effet :

$\begin{cases} \forall m \in IM \\ \exists a_i \in I \end{cases}$ $m = \sum_{i=1}^{p} a_i m_i = \sum_{i=1}^{p} a_i \sum_{j=1}^{n} b_j^i x_j = \sum_{j=1}^{n} \underbrace{\left(\sum_{i=1}^{p} a_i b_j^i\right)}_{\in I} x_j$

Moyennant cette remarque (R), la démonstration de la proposition est facile.

$\forall \dot{x} \in M/_{IM} \qquad \exists\, \lambda_i \in A \;/\; x = \sum_{i=1}^{n} \lambda_i x_i$

d'où $\quad \dot{x} = \sum_{i=1}^{n} \dot{\lambda}_i \dot{x}_i$

ce qui prouve que $(\dot{x}_1, \dots, \dot{x}_n)$ est un système générateur dans $M/_{IM}$.
De plus, c'est une base ! En effet, considérons la combinaison linéaire $\sum_{i=1}^{n} \dot{\lambda}_i \dot{x}_i = \dot{0} \Rightarrow \sum_{i=1}^{n} \lambda_i x_i \in IM \underset{(\text{cf } R)}{\Rightarrow} \lambda_i \in I \;\forall i \Rightarrow \underset{\forall i}{\dot{\lambda}_i = \dot{0}}$

Ce qui prouve que $M/_{IM}$ est <u>libre de type fini</u>.

a)

$\mathfrak{m}$ idéal maximal donc $A/_{\mathfrak{m}}$ est un corps.

$M/_{\mathfrak{m}M}$ est un $A/_{\mathfrak{m}}$ - module. $\Rightarrow$ $M/_{\mathfrak{m}M}$ est un $A/_{\mathfrak{m}}$ - espace vectoriel

<u>Remarque</u>: Dans ce cas où M est un module libre de type fini, on remarque que pour <u>tout</u> $\mathfrak{m}$ idéal maximal, $M/_{\mathfrak{m}M}$ est un corps de dimension n, constante.

<u>mardi 5 février 80</u>

(2) M = A-module $\qquad A$ anneau commutatif.

1°/ <u>Déterminer $Hom_A(A, M)$</u>

Si $\varphi \in Hom_A(A, M)$, on a $\forall a \in A \quad \varphi(a.1) = a\varphi(1)$

d'où $\quad \Psi : \; Hom_A(A, M) \longrightarrow M$
$\qquad\qquad\qquad \varphi \longmapsto \varphi(1)$

Ψ est bijective.
(d'ailleurs, si $x \in M$ est fixé, $\varphi(a) = ax$ est antécédent de x).
Tout cela est très simple.

2°/ <u>$M^* = Hom_A(M, A)$ est un A-module</u> pour les opérations suivantes

$\forall \begin{cases} f, g \in M^* \\ a \in A \end{cases}$ on a $(f+g) \in M^*$ et $af \in M^*$ car : $\begin{cases} (af)(x+y) = a f(x+y) = a f(x) + a f(y) \\ (af)(bx) = a b f(x) = b\, af(x) \text{ car } A \text{ comm.} \end{cases}$

Définition de $M \to M^{**}$

$$h: M \longrightarrow M^{**}$$
$$x \longmapsto \hat{x}(f) = f(x)$$

h est un homomorphisme de A-modules.

Calculons, par exemple $Hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$

En effet, $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \Rightarrow \underbrace{\varphi(n.\dot{1})}_{\varphi(\dot{0})} = n\varphi(\dot{1}) \Rightarrow \varphi(1) = 0$

Donc:
h n'est pas injective, où $h: \mathbb{Z}/n\mathbb{Z} \to \{0\}$.

Si $p|q$, il est clair que $\mathbb{Z}/p\mathbb{Z}$ est un $\mathbb{Z}/q\mathbb{Z}$-module.

Si $p|q$, considérons $Hom_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$. (P)

Remarque : Si $A \xrightarrow{\varphi} B$ est un homomorphisme d'anneaux, et si M est un B-module, alors la multiplication $M \times A \longrightarrow M$, $(m, a) \mapsto \varphi(a)m$ est un A-module, d'une façon canonique.

En utilisant cette remarque, on voit bien que $\mathbb{Z}/p\mathbb{Z}$ est un $\mathbb{Z}/q\mathbb{Z}$-module ($p|q$) pour la multiplication externe

$$\bar{x}.\dot{y} = \dot{\overline{xy}} \quad \text{(bien défini}$$
($\bar{x}$ mod q, $\dot{y}$ mod p)

Solution de (P)

Soit $q = pr$

Notons $(\mathbb{Z}/p\mathbb{Z})^* = Hom_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z})$.

et considérons $\varphi \in (\mathbb{Z}/p\mathbb{Z})^*$.

On a: $\varphi(\bar{y}^p) = \varphi(\bar{1}^q.\bar{y}^p) = \varphi(\bar{1}^q.\bar{y}.\bar{1}^p) = \varphi(\bar{y}^q.\bar{1}^p)$
$= \bar{y}^q\varphi(\bar{1}^p)$

Donc, si $g: (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mathbb{Z}/q\mathbb{Z}$, $\varphi \longmapsto \varphi(\bar{1}^p)$ est
- définie
- injective
- est un homomorphisme de $(\mathbb{Z}/q\mathbb{Z})$-module.

Cherchons Im g.

Soit $\bar{a}^q \in \mathbb{Z}/q\mathbb{Z}$. Cherchons φ / $\varphi(\bar{1}^p) = \bar{a}^q$

~~Or donc~~ $\exists \varphi / \varphi(\bar{1}^p) = \bar{a}^q \iff \exists \varphi / \varphi(\bar{k}^p) = k\bar{a}^q \quad \forall k \in \mathbb{Z}$

$\iff \exists \varphi / \varphi(\bar{0}) = p\bar{a}^q$

$\iff q \mid pa \iff r \mid a$

Ainsi $g((\mathbb{Z}/p\mathbb{Z})^*) = \{ \bar{a}^q \in \mathbb{Z}/q\mathbb{Z} \ / \ r \mid a \}$

$= r(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$

Ainsi

$$\boxed{\mathrm{Hom}_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}}$$

~~(6) 1) $\mathrm{Hom}_A(A^n, A) \simeq A^n$~~ (Suite du TD : feuille 8 de la même série.)

~~2) $u : M \to N$ A-linéaire~~

~~$M^* \xleftarrow{{}^t u} N^*$ / ${}^t u(n^*) = n^* \circ u$~~

I.M.S.P.

MATHEMATIQUES

M 1 ALGEBRE - PARTIEL DU 31 MARS 1978

Durée : 3 HEURES

Les exercices 1, 2, 3, 4 sont indépendants. Leur solution exige plus de réflexion que de connaissances ...

I . Soit $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ un homomorphisme, de matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Donner une CNS sur les entiers a, b, c, d pour que le groupe $\mathbb{Z}^2 / \mathrm{Im}\, f$ soit cyclique. Préciser la structure du groupe $\mathbb{Z}^2 / \mathrm{Im}\, f$ dans le cas de la matrice $\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$.

II . Soit K un corps fini. On choisit au hasard un élément c parmi les éléments de K , supposés équiprobables. Quelle est la probabilité pour que le polynôme $x^2 + x - c = 0$ soit irréductible sur K ? on distinguera les cas car K = 2 , car K ≠ 2 .

III . Soit P un polynôme de degré n à coefficients entiers. On pose

$$Q(X) = P(X + P(X))$$

a/ Quel est le degré de Q ? Il y a un cas particulier !

b/ Montrer que P(X) divise Q(X)

c/ En déduire qu'il n'existe pas de polynôme $P \in \mathbb{Z}[X]$, non constant, tel que :

$$\forall n \in \mathbb{Z} , \quad P(n) \text{ est premier.}$$

IV . Soit $G_p = (\mathbb{Z} / p\mathbb{Z})^*$ le groupe multiplicatif du corps $\mathbb{Z} / p\mathbb{Z}$.

On suppose $p \neq 2$. On rappelle que G_p est cyclique

a/ Soit a un générateur de G_p. Montrer que

$$(a)^{\frac{p-1}{2}} = -1$$

b/ Montrer que $x \in G_p$ est le carré d'un élément $y \in G_p$ si et seulement si :

$$(x)^{\frac{p-1}{2}} = 1 .$$

c/ On considère l'entier

$$A = \prod_{k=1}^{k=\frac{p-1}{2}} (2k) = 2 . 4 \dots (p-3)(p-1) .$$

En distinguant les cas $(\frac{p-1}{2})$ pair, $\frac{p-1}{2}$ impair, montrer que

$$A \equiv (-1)^{u(p)} (\frac{p-1}{2})! \bmod. p$$

où $u(p)$ est une fonction de p que l'on précisera dans chaque cas.

En déduire que $2^{\frac{p-1}{2}} \equiv (-1)^{u(p)}$ et indiquer pour quelles valeurs de p la classe de 2 est un carré dans $\mathbb{Z} / p\mathbb{Z}$

d/ Montrer que $X^3 + X^2 - 3X + 1$ a trois racines dans $\mathbb{Z} / 97 \mathbb{Z}$ (il n'est pas interdit de les chercher).

Partiel du 31 mars 1978

① $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ de matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\exists$ base (e_1, e_2) de $\mathbb{Z}^2$-départ
$\exists$ base (f_1, f_2) de $\mathbb{Z}^2$-arrivée telles que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ (matrice dans les nouvelles bases.)

où $\begin{cases} d_1 = \delta(a,b,c,d) \\ d_1 d_2 = ~~pgcd~~ .\, ad - bc \end{cases}$ et $d_1 | d_2$.

Alors $\operatorname{Im} f \simeq d_1\mathbb{Z} \times d_2\mathbb{Z}$

$$\mathbb{Z}^2/\operatorname{Im} f = \mathbb{Z}^2/d_1\mathbb{Z} \times d_2\mathbb{Z} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

NB : Ici cyclique $\Leftrightarrow$ monogène (pas forcément fini)

- Si $d_1 = d_2 = 0$ $f = 0 \Rightarrow \operatorname{Im} f = \{0\}$ d'où $\mathbb{Z}^2/\operatorname{Im} f \simeq \mathbb{Z}^2$ non cyclique.
- Si $d_2 = 0$ $\mathbb{Z}^2/\operatorname{Im} f \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}$ $(d_1 \neq 0)$

S'il était cyclique, il existerait un isomorphisme de groupe de $\mathbb{Z}^2/\operatorname{Im} f$ sur $\mathbb{Z}/n\mathbb{Z}$ ou sur $\mathbb{Z}$. Si $\varphi : \mathbb{Z}^2/\operatorname{Im} f \to \mathbb{Z}/n\mathbb{Z}$, on aurait un élément [à savoir $(\dot{0}, 1) \in \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}$] d'ordre infini. Donc $\varphi : \mathbb{Z}^2/\operatorname{Im} f \to \mathbb{Z}$. Mais, de la m̂ façon, il y aurait un élément d'ordre fini sauf si $d_1 = 1$. Donc $\mathbb{Z}^2/\operatorname{Im} f$ non cyclique.

- Si d_1 et d_2 non nuls , $\mathbb{Z}^2/\operatorname{Im} f \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$

~~Si~~ $\delta(d_1, d_2) = 1 \Leftrightarrow \mathbb{Z}^2/\operatorname{Im} f \simeq \mathbb{Z}/d_1 d_2\mathbb{Z}$ (th. Chinois)

Ainsi $\mathbb{Z}^2/\mathrm{Im} f$ cyclique $\Leftrightarrow$ $\omega(d_1, d_2) = 1 \Leftrightarrow d_1 = 1$ (car $d_1 | d_2$)

Cas de $M = \begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$

$$\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix} \sim ~~\begin{pmatrix} 0 & 12 \\ -6 & 0 \end{pmatrix}~~ \begin{pmatrix} 2 & 4 \\ 0 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

$\mathbb{Z}^2/\mathrm{Im} f \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ non cycliques.

(2) K = corps fini.

$c \in K$ $\qquad x^2 + x - c = 0$ irréductible sur K

③ $P \in \mathbb{Z}[X]$ $\quad Q(X) = P(X + P(X))$

a) * Si $\deg P \geqslant 2$ $\quad \deg Q(X) = (\deg P)^2$

* Si $\deg P = 1$ $\quad \begin{cases} \deg Q = 1 & \text{si } P \neq -X + \text{cte} \\ \deg Q = 0 & \text{si } P = -X + \text{cte} \end{cases}$

* Si $\deg P = 0$, $\deg Q = 0$.

Ainsi :

$$\boxed{\deg Q = (\deg P)^2 \text{ sauf si } P = -X + \text{cte, auquel cas } \deg Q = 0}$$

b) <u>$P(X)$ divise $Q(X)$</u> $\qquad$ 1^{re} <u>méthode</u>

$P \in \mathbb{Z}[X] \subset \mathbb{C}[X]$

Soit $\alpha \in \mathbb{C}$ / $P(\alpha) = 0$. Alors $Q(\alpha) = P(\alpha + P(\alpha)) = 0$

Toute racine de P est racine de Q. Cela n'est pas suffisant pour affirmer que $P | Q$. Montrons que :

α racine de P de multiplicité k $\Rightarrow$ α rac. de Q de mult. k au moins. $\quad$ (R)

Alors, si (R) est prouvé, on aura : $P | Q$, puisque :

$$\begin{cases} P = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} \\ \text{et} \\ Q = (X - \alpha_1)^{\ell_1} \cdots (X - \alpha_m)^{\ell_m} Q_1(X) \end{cases}$$

<u>Preuve de (R)</u>

<u>Récurrence finie sur l'ordre de α</u>.

Soit α d'ordre $k > 1$ ds $P(X)$; $\mathcal{P}(n) =$ " $(X - \alpha)^n$ divise $Q(X)$ ".

- $\mathcal{P}(1)$ vrai.

• Montrons que $\forall n \in [1, k-1]$ $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ vraie.

On a $\mathcal{P}(n)$ vraie : $(X-\alpha)^n \mid Q(X)$.

Ainsi $\begin{cases} Q(X) = (X-\alpha)^n Q_1(X) \\ \text{Or } P(X) = (X-\alpha)^n P_1(X) \end{cases}$

d'où $Q(X) = P(X+P(X)) \Rightarrow (X-\alpha)^n Q_1(X) = (X+P(X)-\alpha)^n P_1(X+P(X))$

$$\Rightarrow (X-\alpha)^n Q_1(X) = [(X-\alpha)(1+(X-\alpha)^{n-1}P_1(X))]^n P_1(X+P(X))$$

d'où $(X-\alpha)^n Q_1(X) = (X-\alpha)^n (1+(X-\alpha)^{n-1}P_1(X))^n P_1(X+P(X))$

$$Q_1(X) = (1+(X-\alpha)^{n-1}P_1(X))^n P_1(X+P(X))$$

donc $Q_1(\alpha) = P_1(\alpha+P(\alpha)) = P_1(\alpha) = 0$ car $P_1(\alpha) = 0$.

D'où $Q(X) = (X-\alpha)^{n+1} Q_2(X) \Leftrightarrow \mathcal{P}(n+1)$ vraie.

Conclusion : $\mathcal{P}(k)$ vraie, c.à.d $(X-\alpha)^k \mid Q(X)$.

2-méthode

$$\begin{cases} P(X) = \sum_{k=0}^{n} a_k X^k \\ Q(X) = \sum_{k=0}^{n} a_k (X^k + P(X).R_k(X)) \end{cases}$$ et rac ! ?

c) $P \in \mathbb{Z}[X]$ / $\forall n \in \mathbb{Z}$ $P(n)$ premier $\Rightarrow$ $P = \text{cte} \in \mathbb{Z}$

Si P convient, alors $P(n) \mid Q(n)$ et $Q(n) = P(n + P(n))$ premier.

Donc $P(n) = Q(n)$ $\forall n \in \mathbb{N}$ (car $P(n) \neq 1$)

$R(X) = P(X) - Q(X)$ possède alors une infinité de racine. Tout polynôme de $\mathbb{Z}[X]$ de degré n admet au plus n racines (car $\mathbb{Z}$ anneau com. et intègre). Donc $P(X) = Q(X) \Rightarrow \begin{cases} (\deg P)^2 = \deg P \text{ et } P \neq -X + \text{cte} \\ \text{ou} \\ 0 = \deg P \text{ et } P = -X + \text{cte}, \text{imp.} \end{cases}$

$P(X) = Q(X) \Rightarrow [\deg P = 1 \text{ ou } \deg P = 0 \text{ et } P \neq -X + \text{cte}]$

$$\Rightarrow \begin{cases} \deg P = 0 & (1) \\ \text{ou} \\ \deg P = 1 \text{ et } P \neq -X + \text{cte} & (2) \end{cases}$$

Montrons que le (2) ne peut pas se produire. Supposons que $P(X) = aX + b$ où $a \neq 0$ et $a \neq -1$.

$P(X + P(X)) = a(a+1)X + ab + b = P(X) = aX + b$

$$\Downarrow$$

$$a = a(a+1)$$

$$\Downarrow$$

$$1 = a + 1$$

$$\Downarrow$$

$a = 0$ non

Ainsi

$P \in \mathbb{Z}[X]$ / $\forall n \in \mathbb{Z}$ $P(n)$ premier $\Rightarrow$ $P = \text{cte} \in \mathbb{Z}$

CQFD

(4) $G_p = \mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ où p premier. $p \neq 2$.

a) a générateur de $G_p \Leftrightarrow \begin{cases} a^{p-1} = 1 \\ a^k \neq 1 & \forall k \in [1, p-2] \end{cases}$

Posons $p = 2p' + 1$.

Ainsi $a^{p-1} = 1 \Leftrightarrow (a^{p'})^2 = 1 \Rightarrow a^{p'} = \pm 1$

Comme $a^{p'} \neq 1$, $a^{p'} = -1$.

b) $x \in G_p$ $\{ x = y^2 \Leftrightarrow x^{p'} = 1 \}$

Si $x = y^2$ alors $x^{p'} = y^{2p'} = y^{p-1} = 1$ oui.

Inversement, si $x^{p'} = 1$, $x = a^k$ où a générateur de G_p.

$a^{kp'} = 1 \Rightarrow (a^{p'})^k = 1 \Rightarrow (-1)^k = 1 \Rightarrow k \equiv 0 \ [2]$

d'où $k = 2k'$ $x = (a^2)^{k'}$

c) $A = \prod_{k=1}^{k=p'} (2k) = 2 \cdot 4 \cdots (p-3)\underbrace{(p-1)}_{2p'}$ $p' = \frac{p-1}{2}$

$A \equiv (-1)^{u(p)}$ ~~$(p-1)$~~ $(p')!$ $[p]$

Si $\frac{p-1}{2}$ pair

$A = 2 \times 4 \times 6 \cdots \times p' \times \overbrace{(p'+2)}^{\equiv 1 - p' \ [p]} \times \cdots \times \underbrace{(p-1)}_{\equiv (-1) \ [p]} \equiv$ ~~$2 \times 4 \times \cdots \times p' \times (2 + p' - p) \times \cdots \times (-1)$~~

~~$\equiv p' [p]$~~

$A = ~~2 \times 4 \times \dots \times p' \times (p'-(p+2))~~ \times \dots \times (-1)$

$~~(-1)(p+2-p') \times \dots \times~~ (-1)$

$\frac{p'}{2}$ terms.

$$A = (-1)^{\frac{p'}{2}} (p')!$$

$\frac{p-1}{2}$ impair $\quad p = 2p'+1$

$$A = \underbrace{2 \times 4 \times 6 \times \dots \times (p'-1)}_{\frac{p'-1}{2} \text{ terms.}} \times \overbrace{(p'+1)}^{\equiv -p' [p]} \times \underbrace{(p'+2)}_{\equiv 3-p' [p]} \times \dots \times \underbrace{(p-1)}_{\equiv -1 [p]}$$

$$A = (-1)^{\frac{p'-1}{2}} (p')!$$

$$\begin{cases} \text{Si } \frac{p-1}{2} \text{ pair} & u(p) = (-1)^{\frac{p-1}{4}} \\ \text{Si } \frac{p-1}{2} \text{ impair} & u(p) = (-1)^{\frac{p-3}{4}} \end{cases}$$

$$A = 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \Rightarrow 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \equiv \left(\frac{p-1}{2}\right)! (-1)^{u(p)} [p]$$

$$\Downarrow$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{u(p)} [p]$$

($\mathbb{Z}/p\mathbb{Z}$ intègre)

2 est un carré dans $\mathbb{Z}/p\mathbb{Z} \iff 2^{\frac{p-1}{2}} \equiv 1 \iff (-1)^{u(p)} \equiv 1 \quad [p]$

$\iff u(p)$ pair (1)

$$\begin{cases} \text{Si } \frac{p-1}{2} \text{ pair}, & (1) \iff \frac{p-1}{4} \equiv 0 \ [2] \iff p-1 = 8k \iff p \equiv 1 \ [8] \quad (2) \\ \text{Si } \frac{p-1}{2} \text{ impair}, & (1) \iff \frac{p-3}{4} \equiv 0 \ [2] \iff p-3 = 8k \iff p \equiv 3 \ [8] \quad (3) \end{cases}$$

$$\begin{cases} (3) : \text{Si } p = 3+8k \quad \frac{p-1}{2} = \frac{2+8k}{2} = 1+4k \quad \text{pas de contradiction} \\ (2). \end{cases}$$

d) $X^3 + X^2 - 3X + 1 = 0$

$\mathbb{Z}/97\mathbb{Z}$

$(X-1)(X^2 + \alpha X - 1)$ où $\alpha = ~~\cdot~~ 2$

$(X-1)(X^2 + 2X - 1) = 0$

$\Updownarrow$

~~$(X-1)(X-1)^2 = 0$~~

$$\begin{cases} X = 1 \\ \text{ou} \\ X^2 + 2X - 1 = 0 \end{cases}$$

$X^2 + 2X - 1 = (X+1)^2 - 2 = 0$

$\Updownarrow$

$(X+1)^2 = 2$

$\exists$ 2 sol à cette équation ssi 2 est un carré dans $\mathbb{Z}/97\mathbb{Z}$. $\frac{97-1}{2} = 48$ pair

faire exo 163 et 164 p296

Exercice

Montrer que $\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)$ (1)

1°/ 1re méthode

Introduire $I = E_1 \cap E_2$ et $\begin{cases} F_1 \oplus I = E_1 \\ F_2 \oplus I = E_2 \end{cases}$ etc...

2°/ 2e méthode

a) On considère $f : E_1 \times E_2 \to E$
$(x_1, x_2) \mapsto x_1 + x_2$

Montrer que f est linéaire

b) Montrer que $\ker f = \{(x, -x) \ / x \in E_1 \cap E_2\}$
En déduire que $\ker f$ est isomorphe à $E_1 \cap E_2$

c) Démontrer que $\operatorname{Im} f = E_1 + E_2$
En déduire que l'on a la formule (1)

Sol

1°/

Posons $I = E_1 \cap E_2$

$\begin{cases} I \oplus F_1 = E_1 \\ I \oplus F_2 = E_2 \end{cases}$

d'où :

$\begin{cases} \dim I + \dim F_1 = \dim E_1 \\ \dim I + \dim F_2 = \dim E_2 \end{cases}$

$\dim F_1 + \dim F_2 + \dim(E_1 \cap E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)$

Montrons que $F_1 \oplus F_2 \oplus (E_1 \cap E_2) = E_1 + E_2$

Soit $x = \underbrace{x_1}_{\in E_1} + \underbrace{x_2}_{\in E_2}$, alors $x = x_1^I + x_1^{F_1} + x_2^I + x_2^{F_2}$

$x = \underbrace{x_1^I + x_2^I}_{\in I} + \underbrace{x_1^{F_1}}_{\in F_1} + \underbrace{x_2^{F_2}}_{\in F_2}$

donc $E_1 + E_2 \subset \underbrace{F_1 + F_2 + E_1 \cap E_2}$

de plus, cette somme est directe car :

$$\begin{cases} F_1 \cap F_2 \cap (E_1 \cap E_2) = \{\vec{0}\} \\ \text{et} \\ F_1 \cap F_2 = \{\vec{0}\} \end{cases}$$

d'où $E_1 + E_2 \subset F_1 \oplus F_2 \oplus E_1 \cap E_2$

Inversement, soit $x = \underbrace{x_1}_{\in F_1} + \underbrace{x_2}_{\in F_2} + \underbrace{x_I}_{\in E_1 \cap E_2} \in F_1 \oplus F_2 \oplus E_1 \cap E_2$

Alors $x = \underbrace{x_1 + \frac{x_I}{2}}_{\in E_1} + \underbrace{x_2 + \frac{x_I}{2}}_{\in E_2} \Rightarrow x \in E_1 + E_2$

2°/

a) évident

b) $\operatorname{Ker} f = \{(x_1, x_2) \in E_1 \times E_2 \ / \ x_1 = -x_2\}$

$= \{(x, -x) \ / \ x \in E_1 \cap E_2\}$

On exhibe l'isomorphisme d'e.v :

$$\varphi : \begin{array}{ccc} E_1 \cap E_2 & \longrightarrow & \operatorname{Ker} f \\ x & \longmapsto & (x, -x) \end{array}$$

c) $\operatorname{Im} f = E_1 + E_2$ (évident)

Conclusion : $\dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim E_1 \times E_2$

$\dim(E_1 \cap E_2) + \dim(E_1 + E_2) = \dim E_1 + \dim E_2$

$$\boxed{\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)}$$

Queysanne

(1) 163 p 296

$E_0, E_1, \dots, E_n$ = e.v. sur K $(n \geq 1)$

Df :

$$E_0 \xrightarrow{f_0} E_1 \longrightarrow \cdots \longrightarrow E_{k-1} \xrightarrow{f_{k-1}} E_k \xrightarrow{f_k} E_{k+1} \longrightarrow \cdots \xrightarrow{f_{n-1}} E_n$$

est une suite exacte ssi

$$\mathrm{Im}\, f_k = \mathrm{Ker}\, f_{k+1} \qquad \forall k \in [0, n-2]$$

a) $[0 \rightarrow E \xrightarrow{f} F$ est une suite exacte$] \Leftrightarrow f$ injective

$\exists !\, \ell$ linéaire de 0 vers E, à savoir : $\ell(0) = \vec{0}_E$

$(\Leftarrow)$ f injective $\Rightarrow \mathrm{Ker}\, f = \{\vec{0}_E\} \Rightarrow \mathrm{Im}\, \ell = \mathrm{Ker}\, f$.

$(\Rightarrow)$ $\underbrace{\mathrm{Im}\, \ell}_{\{0_E\}} = \mathrm{Ker}\, f \Rightarrow f$ injective.

$[E \xrightarrow{f} F \xrightarrow{\ell} 0$ est une suite exacte $] \Leftrightarrow f$ surjective

En effet : f surjective $\Leftrightarrow f(E) = F = \mathrm{Ker}\, \ell \Leftrightarrow [E \xrightarrow{f} F \xrightarrow{\ell} 0$ exacte $]$

b)

$$0 \xrightarrow{\ell} F \xrightarrow{i} E \xrightarrow{s} E/F \xrightarrow{\ell'} 0$$

$$\begin{cases} \mathrm{Ker}\, i = \{\vec{0}\} & \text{(car } i \text{ inj)} \\ \mathrm{Ker}\, s = F = \mathrm{Im}\, i & \\ \mathrm{Ker}\, \ell' = \mathrm{Im}\, s & \text{(car } s \text{ surj.)} \end{cases}$$

$$0 \xrightarrow{\ell} \mathrm{Ker} f \xrightarrow{i} E \xrightarrow{f} F \xrightarrow{s} F/\mathrm{Im} f \xrightarrow{\ell'} 0$$

$\mathrm{Ker}\, i = \{\vec{0}\}$ car i injective

$\mathrm{Ker}\, \ell' = F/\mathrm{Im} f$ car s surj.

De plus :

* $\text{Ker} f = \text{Im}\, i$
* $\text{Ker}\, s = \{x \in F \,/\, s(x) = \dot{0} \in F/\text{Im} f\}$

$= \{x \in F \,/\, x \in \text{Im} f\}$

$= \text{Im} f$

CQFD

164 p 297

a)

$$0 \longrightarrow E_0 \xrightarrow{f_0} \cdots \longrightarrow E_k \xrightarrow{f_k} E_{k+1} \longrightarrow \cdots \xrightarrow{f_{n-1}} E_n \longrightarrow 0$$

Mq

$$\sum_{2k+1 \leq n} \dim E_{2k+1} = \sum_{2k \leq n} \dim E_{2k} \quad (1)$$

$\forall k \in [0, n-1]$ $\quad \dim \text{Im} f_k + \underbrace{\dim \text{Ker} f_k}_{\dim \text{Im} f_{k-1}} = \dim E_k$

$$(I) \begin{cases} \dim \text{Im} f_0 = \dim E_0 \\ \dim \text{Im} f_1 + \dim \text{Im} f_0 = \dim E_1 \\ \dim \text{Im} f_2 + \dim \text{Im} f_1 = \dim E_2 \\ \cdots \\ \dim \text{Im} f_{n-1} + \dim \text{Im} f_{n-2} = \dim E_{n-1} \\ \dim \text{Im} f_{n-1} = \dim E_n \end{cases}$$

$$\dim E_0 - \dim E_1 + \cdots + (-1)^n \dim E_n = 0 \quad (2)$$

On n'a toujours pas montré (1)

En ajoutant seulement les lignes pairs du système (I),

nous obtenons : * Si n pair

$$\dim E_0 + \dim E_2 + \dots + \dim E_n = \sum_{k=1}^{n-1} \dim \operatorname{Im} f_k$$

et :

$$\dim E_1 + \dim E_3 + \dots + \dim E_{n-1} = \sum_{k=1}^{n-1} \dim \operatorname{Im} f_k$$

d'où l'égalité (1)

* Si n impair : m̂ dem.

Remarque : on peut ne pas considérer de cas n pair ou impair, et se rappeler de f… :

$$2E\left(\frac{n-1}{2}\right) = \begin{cases} n \text{ impair} \rightarrow n-1 \\ n \text{ pair} \rightarrow n \end{cases}$$

b) $0 \rightarrow E \cap F \xrightarrow{f+g} E \oplus F \xrightarrow{i-j} E+F \rightarrow 0$

* c'est une suite exacte

* on en déduit la formule $\dim(E+F) + \dim(E \cap F) = \dim E \oplus F$

UNIVERSITE DE NICE
MATHEMATIQUES

SESSION DE JUIN 1978

M. 1 ALGEBRE - DUREE / 3H

mercredi 14 Juin

I Soit G un groupe, H et K deux sous-groupes de G. Montrer que $G = H \cup K$ entraîne $G = H$ ou $G = K$ (utiliser une partition de G en classes à gauche).

II On considère l'application

$$f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^2$$

$$(x,y,z) \longmapsto (2x - 3y \ , \ x + 6y - 3z)$$

1) Montrer que $\mathbb{Z}^2 / \text{Im } f$ est un groupe cyclique dont on déterminera l'ordre n

2) Définir un homomorphisme surjectif $g : \mathbb{Z}^2 \to \mathbb{Z} / n\mathbb{Z}$ de noyau $\text{Im } f$

3) Déterminer le noyau de f.

4) Résoudre le système

$$2x - 3y = 5$$
$$x + 6y - 3z = 1$$

III Soit E l'ensemble des polynômes de degré $\leq n$, à coefficients rationnels, tels que

$$\forall P \in E \ , \quad \forall m \in \mathbb{Z} \ , \quad P(m) \in \mathbb{Z}$$

Il est clair que E est un sous-groupe de $(\mathbb{Q}[X] \ , +)$

a) En considérant l'application

$$F : E \longrightarrow \mathbb{Z}^{n+1}$$

$$P \longmapsto (P(0) \ , P(1), \ldots, P(n))$$

montrer que E est un groupe abélien libre de rang $\leq n + 1$.

.../...

b) Construire un homomorphisme injectif de Z^{n+1} dans E . Conclure . (On considèrera les polynômes à coefficients entiers) .

c) On considère les polynômes

$$P_0(X) = 1 \ , \ P_1(X) = X \ , \ \ldots\ldots P_k(X) = \frac{X(X-1)\ \ldots\ (X-k+1)}{k!} \ldots$$

pour $0 \le k \le n$.

Soit E' le sous-groupe de E engendré par ces polynômes. Montrer (en étudiant sa matrice) que la restriction de F à E' est une bijection de E' sur Z^{n+1} . Que peut-on en conclure ?

Énoncés

① Déterminer les nombres n pour lesquels $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

② Soit A une $\mathbb{R}$-algèbre commutative, de dimension 2. α) Montrer que A est isomorphe à un quotient $\mathbb{R}[X]/(P)$ où $\deg P = 2$. (on note $(P) = P\,\mathbb{R}[X]$)
β) En discutant sur P, montrer que A est isomorphe à l'une des 3 algèbres suivantes :

* $\mathbb{C}$
* $\mathbb{R}[X]/(X^2)$ ou $\mathbb{R} \oplus \mathbb{R}\varepsilon$ (nbres duaux, ou développements limités à l'ordre 2)
* $\mathbb{R}^2$ (loi d'anneau produit)

③ Résoudre $x^3 - 3x + 27 \equiv 0 \quad [1125]$

Solutions

① $n = 2^{\alpha} \prod_{i=1}^{\ell} p_i^{\alpha_i}$ où $p_i \in \mathcal{P}$ et $p_i \neq 2$

On cherche l'existence de k tel que $\mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) \xrightarrow[\sim]{\varphi} (\mathbb{Z}/_{2\mathbb{Z}})^{k}$ $(k \neq 0)$

Si φ existe, $\text{Card}\ \mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) = 2^{k}$

$$\Downarrow$$

$$\varphi(n) = 2^{k}$$

Or $\varphi(n) = 2^{\alpha-1} \prod_{i=1}^{\ell} p_i^{\alpha_i - 1}(p_i - 1)$

$\varphi(n) = 2^{k} \underset{\text{Si } \alpha_i > 1}{\Rightarrow} p_i \mid 2^{k} \underset{\text{(th. Gauss)}}{\Rightarrow} p_i = 2$ ou 1, impossible

Nécessairement, si φ existe, $\alpha_i = 1$.

Supposons donc que $n = 2^{\alpha} \prod_{i=1}^{\ell} p_i$

Nous avons : $\mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) \simeq \mathcal{U}(\mathbb{Z}/_{2^{\alpha}\mathbb{Z}} \times \mathbb{Z}/_{p_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p_\ell\mathbb{Z}})$ (th. Chinois)

$$\wr\wr$$

$$\mathcal{U}(\mathbb{Z}/_{2^{\alpha}\mathbb{Z}}) \times \prod_{i=1}^{\ell} \mathcal{U}(\mathbb{Z}/_{p_i\mathbb{Z}})$$

On sait que :

Rappel

- $\mathcal{U}(\mathbb{Z}/_{2^{\alpha}\mathbb{Z}}) \simeq \mathbb{Z}/_{2^{\alpha-2}\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ si $\alpha \geq 3$
- $\mathcal{U}(\mathbb{Z}/_{2^{2}\mathbb{Z}}) \simeq \mathbb{Z}/_{2\mathbb{Z}}$
- $\mathcal{U}(\mathbb{Z}/_{2\mathbb{Z}}) \simeq \{0\}$
- $\forall p \in \mathcal{P} \setminus \{2\}$ $\mathcal{U}(\mathbb{Z}/_{p\mathbb{Z}}) \simeq \mathbb{Z}/_{\varphi(p)\mathbb{Z}}$.

Donc, si $\boxed{\alpha \geqslant 3}$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^{\ell} \mathbb{Z}/\varphi(p_i)\mathbb{Z} \xrightarrow[\sim]{\varphi} (\mathbb{Z}/2\mathbb{Z})^k$$

Tous les éléments de $(\mathbb{Z}/2\mathbb{Z})^k$ sont d'ordre 1 ou 2.

$\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ est cyclique. Il existe $a \in \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ d'ordre $2^{\alpha-2} > 2$. Donc

$(a, 0, \underbrace{0, \dots, 0}_{\ell \text{ fois}}) \in \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^{\ell} \mathbb{Z}/\varphi(p_i)\mathbb{Z}$ est un élément d'ordre $2^{\alpha-2} > 2$.

ce qui montre qu'il n'y a pas d'$\sim$ φ (qui conserverait les ordres !)

- Si $\alpha > 3$, $\nexists \varphi$

Si $\alpha = 3$ $\quad p_i = 3 \Rightarrow$ $n = 2^3 \times 3$, $n = 2^3$ et ça marche, m̂ dem. que ci-dessus

$\boxed{\text{Si } \alpha = 2}$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^{\ell} \mathbb{Z}/(p_i-1)\mathbb{Z} \xrightarrow[\sim]{\varphi} (\mathbb{Z}/2\mathbb{Z})^k$$

On fait encore un argument d'ordres :

$\forall a \in (\mathbb{Z}/2\mathbb{Z})^k \quad \omega(a) = 1$ ou 2.

- $b \in \mathbb{Z}/2\mathbb{Z} \times \prod_1^{\ell} \mathbb{Z}/(p_i-1)\mathbb{Z}$ et $\omega(b) = p_i - 1$

$\Big\} \Rightarrow$ φ existe $\Downarrow$ $p_i - 1 = 1$ ou 2 $\Rightarrow \begin{cases} p_i = 2, \text{ non} \\ \text{ou} \\ p_i = 3. \end{cases}$

Nécessairement, $\underline{p_i = 3}$. (si p_i existe)

Alors $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ convient.

Si $\alpha = 2$: $\begin{cases} n = 2^2 \times 3 \Rightarrow \exists \varphi \ (k=2) \\ n = 2^2 \text{ oui} \\ n \neq 2^2 \times 3 \text{ et } 2^2 \Rightarrow \nexists \varphi \end{cases}$

Si $\alpha = 1$

$$\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_{i=1}^{\ell} \mathbb{Z}/(p_i - 1)\mathbb{Z}$$

De la m façon que précédemment, on montre que φ existe $\Rightarrow p_i = 3$.

Alors, inversement, si $p_i = 3$ $n = 2.3 \Rightarrow \mathcal{U}(\mathbb{Z}/_{2.3\mathbb{Z}}) \simeq (\mathbb{Z}/_{2\mathbb{Z}})^2$ oui.

Si $\alpha = 1$ $n = 2.3 \Rightarrow \exists \varphi \quad (k=2)$
$n \neq 2.3$ et $2 \Rightarrow \nexists \varphi$.

Si $\alpha = 0$

$p_i = 3$ et alors $\mathcal{U}(\mathbb{Z}/_{3\mathbb{Z}}) \simeq \mathbb{Z}/_{2\mathbb{Z}}$.

sa marche.

Ccl $\exists k \in \mathbb{N}^* \,/\quad \mathcal{U}(\mathbb{Z}/_{n\mathbb{Z}}) \simeq (\mathbb{Z}/_{2\mathbb{Z}})^k$

ssi
- $n = 2^3 \times 3$ alors $k = 3$
- $n = 2^3$ alors $k = 2$
- $n = 2^2 \times 3$ alors $k = 2$
- $n = 2^2$ alors $k = 1$
- $n = 2 \times 3$ alors $k = 1$
- $n = 3$ alors $k = 1$

② α) $\mathbb{R}[X] \xrightarrow{\varphi} A$

A un polynôme de $\mathbb{R}[X]$, on peut toujours associer sa valeur en un point d'un $\mathbb{R}$-algèbre.

Soit $(1_A, a)$ une base de $(A, +, .)$

Définissons φ par : $\begin{cases} \varphi(1) = 1 \\ \varphi(X) = a \end{cases}$ et $\boxed{\varphi(P) = P(a)}$

- φ est un morphisme d'algèbre
- φ est surjectif car les 2 éléments de la base sont atteints

$\ker \varphi = \{P \,/\, P(a) = 0\}$ est un idéal de $\mathbb{R}[X]$. Le seul problème est de montrer que $\deg P = 2$. (où $(P) = \ker\varphi$)

$$\begin{array}{ccc} \mathbb{R}[X] & \xrightarrow{\varphi} & A \\ \pi \downarrow & \nearrow \tilde{\varphi} \text{ isomorphisme d'ev.} & \\ \mathbb{R}[X]/(P) & & \end{array}$$

$\dim \mathbb{R}[X]/(P) = \dim A \Rightarrow \boxed{\deg P = 2}$ (cf. Th.)

Th	k corps, $P \in k[X]$ Alors $\dim_k k[X]/(P) = \deg P$

(Sol : exhiber une base $(\dot{1}, \dots, \dot{X}^{n-1})$)

β)

$\mathbb{C}$, $\mathbb{R}\times\mathbb{R}$, où $(a,b)(a',b') = (aa', bb')$

$\mathbb{R} \oplus \mathbb{R}\varepsilon = \mathbb{R}\times\mathbb{R}$ où $(a,b)(a',b') = (aa', ab' + a'b)$

$\begin{cases} (1,0) = 1 \\ (0,1) = \varepsilon \end{cases}$ $a + b\varepsilon$ $\varepsilon^2 = 0$

(cf. les développements limités : pour en faire le produit on le fait d'abord normalement puis on tronque ce qui ce passe. Tronquer ici revient à faire $\varepsilon^2 = 0$)

δ = discriminant de P.

- Si $\Delta > 0$ $\quad P = (X-\alpha)(X-\beta)$ $\quad \alpha \neq \beta$, $\alpha, \beta \in \mathbb{R}$.

$\delta(X-\alpha, X-\beta) = 1 \Rightarrow \mathbb{R}[X]/(P) \simeq_{\text{anneaux}} \mathbb{R}[X]/(X-\alpha) \times \mathbb{R}[X]/(X-\beta)$

(Th. Chinois) $\quad \mathbb{R}[X]/(X-\alpha) \simeq \mathbb{R}$, $Q \mapsto Q(\alpha)$ $\quad \mathbb{R}[X]/(X-\beta) \simeq \mathbb{R}$, $Q \mapsto Q(\beta)$

$\Rightarrow \mathbb{R}[X]/(P) \simeq_{\text{alg}} \boxed{\mathbb{R} \times \mathbb{R}}$

- Si $\delta = 0$ $\quad P = (X-\alpha)^2$ $\quad \mathbb{R}[X]/(P) \simeq \boxed{\mathbb{R}[X]/X^2}$

$\overline{P(X)} \overset{\varphi}{\longmapsto} \overline{P(X+\alpha)}$

- Si $\delta < 0$ $\quad A \simeq \mathbb{C}$

(à continuer.)

Fin

③ $x^3 - 3x + 27 \equiv 0 \quad [1125] \quad (1)$

$1125 = 5^3 \times 3^2$

$x^3 \equiv 0 \ [3] \Rightarrow 3 \mid x^3 \Rightarrow 3 \mid x \quad (3 \in \mathcal{P})$

Posons $x = 3\lambda$

Alors $(1) \Leftrightarrow (2)$; $\quad 3\lambda^3 - \lambda + 3 \equiv 0 \ [5^3]$

et on continue (cf. lecteur qui passe, souviens-toi)

UNIVERSITE DE NICE - MATHEMATIQUES 9H - 12H

M.1 ALGEBRE

3eme PARTIEL

(I) Pour quels couples (a, b) de nombres complexes la matrice

$$\begin{pmatrix} 0 & a \\ a & 2b \end{pmatrix}$$

est-elle diagonalisable ?

(II) Soient A et B deux matrices carrées d'ordre n à coefficients dans le corps commutatif K

1) Montrer que AB et BA sont semblables si A ou B est inversible.

2) En déduire que les polynômes caractéristiques de AB et BA sont égaux - sans hypothèse sur A ou B.

3) Donner un exemple $(n = 2)$ de couple de matrices A et B tel que AB et BA ne soient pas semblables.

(III) Soit V un K-espace vectoriel de dimension n, et soit u un endomorphisme de V. On dira que u est monogène s'il existe un vecteur e de V tel que

$$e_1 = e \quad , \quad e_2 = u(e_1), \ldots, e_k = u(e_{k-1}) , \ldots , e_n = u(e_{n-1})$$

soit une base de V.

1) Montrer que le polynôme minimal d'un endomorphisme monogène est de degré n

2) Etudier la réciproque.

3) Donner un exemple d'endomorphisme non monogène

4) Si $n = 2$, caractériser les endomorphismes non monogènes.

5) Que peut-on dire des valeurs propres (dans une extension convenable de K) d'un endomorphisme monogène diagonalisable ?
Donner des exemples en dimension 3 d'endomorphismes non bijectifs, monogènes et non monogènes.

(IV) Soit M une matrice carrée d'ordre trois sur un corps K de caractéristique convenable. Exprimer le polynôme caractéristique de M en fonction des nombres $\alpha = tr(M)$, $\beta = tr(M^2)$, $\gamma = tr(M^3)$; on précisera le sens de l'adjectif "convenable" utilisé.

1-partiel ALG

UNIVERSITE DE NICE

I.M.S.P. MATHEMATIQUES — PARTIEL DE M.1 ALGEBRE — 21/12/1978

DOCUMENTS AUTORISES

Les exercices I , II , III , IV sont indépendants ; il sera tenu le plus grand compte de la clarté des raisonnements.

I Un ordinateur californien, aidé de quelques étudiants, vient d'établir que le nombre

$$2^{21701} - 1$$

2pts est premier ("le Monde" du 6.12.1978)

Le nombre 21701 est-il premier ?

II

1pts a) La fonction d'Euler $\varphi : \mathbb{N}^* \to \mathbb{N}$ est-elle injective ?

b) Montrer que la fonction

3pts $$n \to n.\varphi(n)$$

est injective. On pourra raisonner par récurrence en divisant par le plus grand nombre premier qui divise n .

III Pour quelles valeurs de n le nombre C_n^k est-il impair pour tout k compris entre 1 et n ?

5pts

IV Soit G le groupe des matrices 2×2 inversibles à coefficients dans le corps $\mathbb{Z} / 3\mathbb{Z}$.

1pt 1/ Montrer que G n'est pas commutatif

2pts 2/ Montrer que l'espace vectoriel $(\mathbb{Z} / 3\mathbb{Z})^2$ sur le corps $\mathbb{Z} / 3\mathbb{Z}$ contient 8 vecteurs non nuls et 4 droites vectorielles. Montrer que $\# G = 48$.

3/ Définir au moyen de l'action évidente de G sur les droites vectorielles un homomorphisme $\rho : G \to \mathfrak{S}_4$

3pts 4/ Montrer que ρ est surjectif. Quel est son noyau ?

2pts 5/ Montrer que tout élément de $\mathfrak{S}_4$ est d'ordre 1,2,3 ou 4 .

6/ En déduire que tout élément de G est d'ordre 1,2,3,4,6 ou 8 . Donner un exemple de matrice de G correspondant à chaque cas.

MATHEMATIQUES — M.1 ALGEBRE ET ARITHMETIQUE — 2e PARTIEL

Jeudi 22 Mars 1979

Les parties I, II, III sont indépendantes. Le mot "entier" désigne un élément de $\mathbb{Z}$.

I a) Déterminer l'ensemble des solutions entières du système :

$$x + y + z = 1$$
$$x + 3y + z = 7$$

b) A quelle condition sur les entiers a, b, c le système

$$x + y + z = \alpha$$
$$ax + by + cz = \beta$$

admet-il des solutions entières quels que soient les entiers α et β ?

c) Existe-t-il des triplets d'entiers (a, b, c) tels que le système

$$\begin{cases} x + y + z = \alpha \\ ax + by + cz = \beta \\ a^2x + b^2y + c^2z = \gamma \end{cases}$$

admette une solution entière quels que soient les entiers (α, β, γ) ?

II a) Ecrire la matrice de la multiplication par X dans la $\mathbb{R}$-base de $\mathbb{R}[X] / (X^2 + 1)^2$ définie par :

$e_1 = 1 \quad e_2 = X \quad e_3 = 1+X^2 \quad e_4 = X(1+X^2)$

b) Soit u un endomorphisme de $\mathbb{R}^4$ dont l'ensemble des valeurs propres dans $\mathbb{C}$ est $\{+i , -i\}$. Montrer qu'il existe une base de $\mathbb{R}^4$ dans laquelle la matrice de u est de la forme

.../...

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

avec $\alpha = 0$ ou $\alpha = 1$. Préciser le polynôme minimal de u dans chaque cas.

III Soit $\mathbb{Q}$ le groupe additif des nombres rationnels, et $\mathbb{Z}$ le sous-groupe des entiers. On considère le groupe $T = \mathbb{Q}/\mathbb{Z}$.

a) Montrer que l'équation $n.x = 0$ admet exactement n solutions dans T , pour tout entier $n \in \mathbb{N}^*$.

b) Montrer que tout sous-groupe fini de T est cyclique .

c) T est-il cyclique ? T est-il de type fini ?

d) Soit n un entier positif non nul donné .
Montrer que l'application

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Q} \\ (x , y) &\longmapsto \frac{xy}{n} \end{aligned}$$

définit par passage au quotient une application biadditive symétrique :

$$f : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow T$$

e) soit C_d le sous-groupe cyclique d'ordre d , d/n (d|n) de $\mathbb{Z}/n\mathbb{Z}$.
Déterminer le sous-groupe :

$$(C_d)^{\perp} = \{\dot{x} \in \mathbb{Z}/n\mathbb{Z} \mid \forall \dot{y} \in C_d \ , \ f(\dot{x},\dot{y}) = 0\}$$

3- partiel ALG

UNIVERSITE DE NICE
I.M.S.P. MATHEMATIQUES

M.1 3ème PARTIEL

1er Juin - 9H-12H

(1) Soit x un nombre complexe algébrique (sur $\mathbb{Q}$). Montrer que ses parties réelles et imaginaires sont algébriques (on rappelle que les nombres algébriques forment un sous-corps de $\mathbb{C}$).

(2) Montrer que $2\cos\frac{\pi}{5}$ et $2\sin\frac{\pi}{5}$ sont respectivement racines des polynômes

$$P_1(X) = X^4 - 3X^2 + 1$$

$$P_2(X) = X^4 - 5X^2 + 5$$

(3) Montrer que P_1 n'est pas irréductible sur $\mathbb{Q}$, mais que P_2 l'est.

(4) Déterminer le groupe de Galois de P_1 (sur $\mathbb{Q}$)

(5) On pose $r_1 = 2\sin\frac{\pi}{5}$, $r_2 = 2\sin\frac{3\pi}{5}$. Quelles sont les racines de P_2 dans $\mathbb{R}$?

(6) Montrer que $\mathbb{Q}(r_1)$ est le corps des racines de P_2. En déduire l'ordre du groupe $\mathrm{Gal}_{\mathbb{Q}}(P_2)$.

(7) Montrer que $r_1 \longmapsto r_2$ définit un élément d'ordre 4 de $\mathrm{Gal}_{\mathbb{Q}}(P_2)$. Conclure.

(8) Montrer (sans calcul) que $r_1^2 + r_2^2 \in \mathbb{Z}$.
En déduire qu'il existe des polynômes $P \in \mathbb{Q}[X]$ tels que

$$P^2 \equiv 5 - X^2 \quad \text{mod. } (X^4 - 5X^2 + 5)$$

et les trouver tous.

NOTE : Le résultat de la question (1) n'est pas utilisé dans la suite.